

明 細 書

著作物保護システム、記録装置、再生装置及び記録媒体

DIGITAL WORK PROTECTION SYSTEM, RECORDING APPARATUS, REPRODUCTION
APPARATUS, AND RECORDING MEDIUM

5

技術分野

本発明は、デジタルデータを大容量の記録媒体に記録し再生する技術に関し、特に不正装置によるコンテンツの不正な記録及び不正な再生を防止する技術に関する。

10

背景技術

近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツ（以下、コンテンツ）を生成して、光ディスク等の大容量記録媒体に格納して配布し、又はネットワークを介して配布するシステムが普及しつつある。

15

配布されたコンテンツは、コンピュータや再生装置等で読み出され、再生、又は複製の対象となる。

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーなどの不正利用を防止するために暗号化技術が用いられる。具体的には、記録装置は、コンテンツを暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する再生装置のみが、記録媒体から読み出した暗号化コンテンツをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる。

20

なお、コンテンツを暗号化して記録媒体に記録する際には、再生装置が保有する復号鍵に対応する暗号化鍵を用いて、コンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、再生装置が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等が用いられる。

25

このとき、再生装置が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による当該再生装置内部の不正な解析により、復号鍵が外部に暴露される危険性がある。復号鍵が一旦不正者により暴露されてしまうと、前記不正者は、コンテンツを不正利用する記録装置、再生装置を製造して不法に販売したり、又はコンテンツを不正利用するためのコンピュータプログラムを作成し、インターネット等によりこのようなプログラムを流布することが考えられる。

このような場合、著作権者は一旦暴露された復号鍵では、次から提供するコンテンツを扱えないようにしたいと考える。このようなことを実現する技術を鍵無効化技術と呼び、特許文献1により鍵無効化を実現するシステムが開示されている。

従来の鍵無効化技術では、予め、記録媒体の書き換え不可領域に、装置の保有する鍵が無効化されていることを示す鍵無効化情報を記録している。装置は、記録媒体に記録されている鍵無効化情報を用いて、当該装置の保有する鍵が無効化されているか否かを判断し、無効化された鍵を保有する場合には、当該装置は、前記記録媒体を利用することができないようにしている。また、新たに鍵の無効化が発生すると、前記の鍵無効化情報は更新され、この無効化発生以降に製造される新たな記録媒体には更新後の鍵無効化情報が記録される。こうして無効化された鍵では新たな記録媒体を利用できない仕組みとなっている。

一方、光ディスク等の記録媒体に記録されているコンテンツの読み出し、あるいは書き込みは、光ディスクドライブと称されるパソコン周辺機器で行われることが一般的であるが、機器の互換性を達成するためにその入出力の方法は公開の情報として標準化され、秘密にされないことが一般的である。このため、記録媒体に記録されているコンテンツは、パソコン等により、容易に読み出すことが可能であり、また、読み出したデータを他の記録媒体に書き込むことも容易である。したがって、コンテンツの著作権を保護するシステムにおいては、記録媒体上のデータを読み出し、他の記録媒体に書き込むという、通常のユーザが行い得る行為に対して、それを防止する有効な機能を備えるシステムでなければならない。記録媒体から読み出したデータが他の記録媒体に書き込まれることを防止する技術をメディアバインド技術と呼び、特許文献2により、メ

メディアバインドを実現するメカニズムが開示されている。

従来のメディアバインド技術を利用して著作権保護を実現するために、予め、記録媒体の書き換え不可領域には、記録媒体を識別する媒体識別子が記録されており、当該記録媒体に記録されている暗号化コンテンツは、この媒体識別子に基づいて、暗号化されている。従って、暗号化コンテンツだけを他の記録媒体に複製しても、他の記録媒体は、別の媒体識別子を記録しており、この別の媒体識別子に基づいて、暗号化コンテンツを正しく復号することはできない。

(発明が解決しようとする課題)

しかしながら、コンテンツの不正な利用の拡大を防ぐために、多様な不正防止技術の実現が要望されている。

(特許文献1)

特開2002-281013号公報

(特許文献2)

特許第3073590号公報

15 (特許文献3)

特開平09-160492号公報

発明の開示

本発明は、上記の要望に対処するために、コンテンツの不正利用を防止することができる著作物保護システム、記録装置、記録方法、再生装置、再生方法、コンピュータプログラム及び記録媒体を提供することを目的とする。

上記目的を達成するために本発明は、記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムである。

25 前記複数の再生装置のうちいずれか1台以上は、無効化されている。

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されている。

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置の

デバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出手段と、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成手段と、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化手段と、前記記憶手段から前記メディア鍵データを読み出す読出手段と、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込手段とを備えている。

5

各再生装置は、前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出手段と、当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号手段と、生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御手段と、復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段とを備える。

15

(発明の効果)

この構成によると、前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記録媒体に書き込み、また、媒体固有番号及びメディア鍵に基づいて、生成された暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、生成された暗号化コンテンツを記録媒体に書き込む。また、再生装置は、デバイス鍵を用いて、暗号化メディア鍵を復号して復号メディア鍵を生成し、生成した復号メディア鍵が、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止する。

25

このように構成されているので、無効化された再生装置を排除することがで

30

きる。

ここで、別の記録媒体は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の別の暗号化メディア鍵から構成される別のメディア鍵データを記憶している。前記記録装置は、さらに、前記別の記録媒体に記憶されている別のメディア鍵データと、前記記憶手段に記憶されている前記メディア鍵データとの新旧を比較する比較手段と、前記別のメディア鍵データの方が新しいと判断される場合に、前記別の記録媒体から前記別のメディア鍵データを読み出し、読み出した前記別のメディア鍵データを、前記記憶手段に記憶されている前記メディア鍵データに、上書きする更新手段とを備え、前記読出手段は、前記メディア鍵データの読出しに代えて、前記記憶手段から前記別のメディア鍵データを読み出し、前記書込手段は、前記メディア鍵データの書込みに代えて、読み出された前記別のメディア鍵データを前記記録媒体の前記書換可能領域に書き込む。

この構成によると、記録装置は、内部に記憶しているメディア鍵データを、別の記録媒体から取得した別の暗号化メディア鍵に更新することができる。

ここで、前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記記録装置は、さらに、前記無効化データに対してデジタル署名を施して検証情報を生成する署名生成手段を備え、前記書込手段は、さらに、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込む。

また、前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記無効化データに対してデジタル署名を施して検証情報を生成し、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込み、前記読出手段は、さらに、前記記録媒体の前記書換可能領域に書き込まれた前記検証情報を読み出し、前記再生装置は、さらに、読み出した前記検証情報に基づいて、署名検証を施して、検証の成功又は失敗を示す検証結果を出力する検証手段を備え、前記制御手段は、さらに、前記検証結果が検証の失敗を示す場合に、前記暗号化コンテンツの復号を禁止し、前記検証結果が検証の成功を示

す場合に、前記暗号化コンテンツの復号を許可する。

この構成によると、記録装置は、さらに、デジタル署名により生成した検証情報を記録媒体に書き込むので、再生装置において、検証情報を検証することにより、不正な再生装置を排除することができる。

- 5 ここで、前記記憶手段は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、前記書込手段は、読み出された前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込む。また、前記記録装置は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記公開鍵証明書を読み出し、読み出した前記公開
- 10 鍵証明書を前記記録媒体の前記書換可能領域に書き込み、前記再生装置は、さらに、前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第1無効化データを記憶している記憶手段と、前記記録媒体から前記公開鍵証明書を読み出す証明書読出手段と、読み出した公開鍵証明書に含まれる公開鍵が、前記第1無効化データにより、無効化され
- 15 ていることを示しているか否かを検証する公開鍵検証手段とを含み、前記制御手段は、さらに、前記公開鍵が無効化されている場合に、前記暗号化コンテンツの復号を禁止し、前記公開鍵が無効化されていない場合に、前記暗号化コンテンツの復号を許可する。

- この構成によると、記録装置は、公開鍵証明書を記録媒体に書き込み、再生
- 20 装置は、記録媒体から公開鍵証明書を読み出し、公開鍵が無効化されている場合に、暗号化コンテンツの復号を禁止できる。

- ここで、別の記録媒体は、前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第2無効化データを記憶しており、前記再生装置は、さらに、前記別の記録媒体に記憶されている前
- 25 記第2無効化データと、前記記憶手段に記憶されている前記第1無効化データとの新旧を比較する比較手段と、前記第2無効化データの方が新しいと判断される場合に、前記別の記録媒体から前記第2無効化データを読み出し、読み出した前記第2無効化データを、前記記憶手段に記憶されている前記第1無効化データに、上書きする更新手段とを含む。

- 30 この構成によると、再生装置は、無効化データを最新の状態に更新すること

ができる。

ここで、前記記憶手段は、さらに、当該記録装置を識別する装置識別子を記憶しており、前記記録装置は、さらに、前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記コンテンツに電子透かしとして埋め込む埋込手段を備え、前記暗号化手段は、前記装置識別子が埋め込まれたコンテンツを暗号化する。また、前記再生装置は、さらに、当該再生装置を識別する装置識別子を記憶している前記記憶手段と、復号が許可された場合に、前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記暗号化コンテンツに電子透かしとして埋め込む埋込手段と、前記装置識別子が埋め込まれた前記暗号化コンテンツを前記記録媒体に書き込む。

記録装置及び再生装置は、装置識別子が埋め込まれたコンテンツを記録媒体に書き込むので、前記コンテンツが不正に流通した場合に、前記コンテンツから、埋め込まれた装置識別子を抽出することにより、そのコンテンツを記録した記録装置及び再生装置を特定することができる。

ここで、前記記憶手段に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、前記書込手段は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込む。また、前記記録装置に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、前記記録装置は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込み、前記再生装置は、さらに、前記記録媒体に記録されている前記暗号化コンテンツの指定を受け付ける受付手段と、指定が受け付けられた前記暗号化コンテンツに対応付けられた前記データ識別子を前記記録媒体から読み出す読出手段と、読み出した前記データ識別子を含む前記メディア鍵データを前記記録媒体から読み出す読出手段とを含み、前記制御手段は、読み出した前記メディア鍵データに基づいて、前記暗号化コンテンツの復号の可否を判断する。

記録装置は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前

記記録媒体^{a)}に書き込み、前記データ識別子を含む前記メディア鍵データを前記記録媒体に書き込むので、再生装置において、データ識別子を介して、暗号化コンテンツに対応するメディア鍵データを取得し、取得したメディア鍵データに基づいて、暗号化コンテンツの復号の可否を判断できる。

5

図面の簡単な説明

図1は、コンテンツ供給システム10の構成を示す構成図である。

図2は、記録装置100の構成を示すブロック図である。

図3は、記録媒体120に記録されているデータの構造を示すデータ構造図
10 である。

図4は、再生装置200の構成を示すブロック図である。

図5は、記録装置100による記録媒体120へのデータの書き込みの動作を示すフローチャートである。

図6は、再生装置200による記録媒体120に記録されているデータの再生の動作を示すフローチャートである。図7へ続く。
15

図7は、再生装置200による記録媒体120に記録されているデータの再生の動作を示すフローチャートである。図6から続く。

図8は、第1の実施の形態の変形例におけるn枚の記録媒体に記録されているデータの構造を示すデータ構造図である。

図9は、第1の実施の形態の変形例における記録媒体に記録されているデータの構造を示すデータ構造図である。
20

図10は、コンテンツ供給システム20の構成を示す構成図である。

図11は、記録装置1100の構成を示すブロック図である。

図12は、記録媒体1300に記録されているデータの構造を示すデータ構造図である。
25

図13は、再生装置1200の構成を示すブロック図である。

図14は、記録媒体1300aに記録されているデータの構造を示すデータ構造図である。

図15は、記録媒体1300bに記録されているデータの構造を示すデータ構造図である。
30

図16は、記録装置1100による記録媒体1300へのデータの書き込みの動作を示すフローチャートである。図17へ続く。

図17は、記録装置1100による記録媒体1300へのデータの書き込みの動作を示すフローチャートである。図18へ続く。

5 図18は、記録装置1100による記録媒体1300へのデータの書き込みの動作を示すフローチャートである。図17から続く。

図19は、再生装置1200による記録媒体1300に記録されているデータの再生の動作を示すフローチャートである。図20へ続く。

10 図20は、再生装置1200による記録媒体1300に記録されているデータの再生の動作を示すフローチャートである。図19から続く。

発明を実施するための最良の形態

1. 第1の実施の形態

15 本発明に係る1の実施の形態としてのコンテンツ供給システム10について説明する。

1. 1 コンテンツ供給システム10の構成

20 コンテンツ供給システム10は、図1に示すように、コンテンツサーバ装置500、記録装置100及び再生装置200a、200b、200c、200d、200e、・・・から構成されている。記録装置100及び再生装置200a、200b、200c、200d、200e、・・・の台数の合計は、n台である。記録装置100には、装置番号「1」が割り当てられており、再生装置200a、200b、200c、200d、200e、・・・には、それぞれ、装置番号「2」、「3」、「4」、・・・、「n」が割り当てられている。各装置は、割り当てられた各装置番号により識別される。

25 これらのn台の装置のうち、再生装置200b及び再生装置200cは、不正な第三者による不正な攻撃を受けたために、本来秘密に内蔵すべき鍵が暴露されており、このため、再生装置200b及び再生装置200cは、無効化されている。

30 音楽や映画などのコンテンツの供給業者は、コンテンツサーバ装置500及び記録装置100を有しており、コンテンツサーバ装置500と記録装置100

0とは、専用回線30を介して接続されている。

コンテンツサーバ装置500は、コンテンツ及び前記コンテンツを暗号化する際に用いられるコンテンツ鍵を有しており、記録装置100からの要求により、コンテンツ及び対応するコンテンツ鍵を、専用回線30を介して、記録装置100へ送信する。

記録装置100は、コンテンツサーバ装置500から、専用回線30を介して、コンテンツ及び対応するコンテンツ鍵を受信し、受信したコンテンツとコンテンツ鍵を暗号化し、暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報をして記録媒体120に書き込む。

暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報が記録された記録媒体120は、販売店で売られ、利用者は、記録媒体120を購入する。

利用者の有する再生装置200aは、記録媒体120が装着されると、記録媒体120から暗号化コンテンツ、暗号化コンテンツ鍵及びその他の関連する情報を読み出し、読み出したその他の関連する情報を用いて、コンテンツの復号の可否を判断し、復号可能であると判断する場合に、暗号化コンテンツ鍵から復号コンテンツ鍵を生成し、復号コンテンツ鍵を用いて復号コンテンツを生成し、生成した復号コンテンツから映画や音楽を生成し、出力する。

1. 2 コンテンツサーバ装置500

コンテンツサーバ装置500は、情報記憶部501、制御部502、入力部503、表示部504及び送受信部505から構成されている（図示していない）。

コンテンツサーバ装置500は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、通信ユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、コンテンツサーバ装置500の各構成要素は、その機能を達成する。

送受信部505は、専用回線30を介して、記録装置100に接続されてお

り、記録装置100と制御部502との間で情報の送受信を行う。

情報記憶部501は、映像情報及び音声情報が高効率で圧縮符号化されて生成されたコンテンツと当該コンテンツを暗号化する際に鍵として用いられるコンテンツ鍵との組を複数個予め記憶している。

- 5 制御部502は、記録装置100から、専用回線30及び送受信部505を介して、いずれかのコンテンツの取得要求を受け取る。前記取得要求を受け取ると、制御部502は、情報記憶部501から、前記取得要求により示されるコンテンツ及びコンテンツ鍵を読み出し、読み出したコンテンツ及びコンテンツ鍵を、送受信部505及び専用回線30を介して、記録装置100へ送信する。

入力部503は、コンテンツサーバ装置500の操作者の指示を受け付け、受け付けた指示を制御部502へ出力する。

表示部504は、制御部502の制御により、様々な情報を表示する。

1. 3 記録装置100

- 15 記録装置100は、図2に示すように、デバイス鍵格納部101、メディア鍵データ格納部102、鍵計算部103、鍵計算部104、暗号化部105、暗号化部106、秘密鍵格納部107、証明書格納部108、CRL格納部109、署名生成部110、ドライブ部111、制御部112及び送受信部113から構成されている。

- 20 記録装置100は、具体的には、コンテンツサーバ装置500と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、記録装置100は、その機能を達成する。

(1) デバイス鍵格納部101

- デバイス鍵格納部101は、外部の装置からアクセスできないように、デバイス鍵DK__1を秘密に記憶している。デバイス鍵DK__1は、記録装置100に固有の鍵である。なお、本明細書において、装置mが保有するデバイス鍵をDK__mと表現している。

(2) メディア鍵データ格納部102

メディア鍵データ格納部102は、メディア鍵データMDATAを記憶している。メディア鍵データMDATAは、n個の組を含み、各組は、暗号化メディア鍵及び装置番号から構成されている。各組に含まれている暗号化メディア鍵と装置番号とは対応している。ここで、nは、上述したように、記録装置100及び再生装置200a、200b、・・・の台数の合計値である。

n個の組のうち、第1の組は、第1の暗号化メディア鍵及び装置番号「1」から構成されている。装置番号「1」は、記録装置100を識別する識別情報である。第1の暗号化メディア鍵は、装置番号「1」により識別される装置、つまり、記録装置100に割り当てられたデバイス鍵DK_1を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

第1の暗号化メディア鍵=E1 (DK_1, MK)

ここで、暗号化アルゴリズムE1は、一例として、DES (Data Encryption Standard) によるものである。また、E (A, B) は、鍵Aを用いて、平文Bに対して暗号化アルゴリズムEを施して得られた暗号文を示している。

また、メディア鍵MKは、記録媒体120に固有の鍵である。

また、n個の組のうち、第2の組は、それぞれ、第2の暗号化メディア鍵及び装置番号「2」から構成されている。ここで、装置番号「2」は、再生装置200aを識別する。また、第2の暗号化メディア鍵は、装置番号「2」の装置、つまり、再生装置200aに割り当てられたデバイス鍵DK_2を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

第2の暗号化メディア鍵=E1 (DK_2, MK)

また、n個の組のうち、第3、第4の組は、それぞれ、第3の暗号化メディア鍵及び装置番号「3」、第4の暗号化メディア鍵及び装置番号「4」から構成されている。ここで、装置番号「3」及び「4」は、それぞれ、再生装置200b、200cを識別する。また、第3、第4の暗号化メディア鍵は、それぞれ、装置番号「3」、「4」により識別される装置、つまり、再生装置200b、200cに割り当てられたデバイス鍵DK_3、DK_4を用いて、メディア鍵MKの代わりに、値「0」に暗号化アルゴリズムE1を施して生成されたものである。

第3の暗号化メディア鍵=E1 (DK_3, 0)

第4の暗号化メディア鍵=E1 (DK_4, 0)

ここで、値「0」は、メディア鍵(MK)とは全く無関係のデータである。
メディア鍵MKの代わりに、値「0」を用いるのは、第3及び第4の暗号化メ
5 デディア鍵に、それぞれ、対応する再生装置200b及び200cが無効化され
ているからであり、再生装置200b及び200cが無効化されていることを
知るための検知情報として用いられる。

無効化された装置について、無効化された装置のデバイス鍵を用いて、メデ
ィア鍵MKとは全く無関係のデータ、つまり値「0」を暗号化して暗号化メデ
10 オディア鍵を生成することにより、無効化された装置以外の全ての装置だけがメデ
ィア鍵MKを共有できる。また、無効化された装置をこのシステムから排除す
ることができる。

ここで、値「0」を用いるとしているが、メディア鍵MKとは、全く無関係
の他のデータであるとしてもよい。例えば、他の固定値である「0xFFFF」、
15 暗号化メディア鍵を生成する時点の日付や時刻を示す情報、当該無効化された
装置のデバイス鍵などであるとしてもよい。

なお、装置の無効化方法は他の方法を利用してもよく、例えば、特許文献1
には木構造を利用した無効化方法が開示されている。

また、n個の組のうち、第5、・・・、第nの組は、それぞれ、第5の暗号
20 化メディア鍵及び装置番号「5」、・・・、第nの暗号化メディア鍵及び装置
番号「n」から構成されている。ここで、装置番号「5」、・・・、「n」は、
それぞれ、再生装置200d、200e、・・・を識別する。また、第5、・・・、
第nの暗号化メディア鍵は、それぞれ、装置番号「5」、・・・「n」の装置、
つまり、再生装置200d、200e、・・・に割り当てられたデバイス鍵D
25 K_5、・・・、DK_nを用いて、メディア鍵MKに暗号化アルゴリズムE
1を施して生成されたものである。

第5の暗号化メディア鍵=E1 (DK_5, MK)

・・・

第nの暗号化メディア鍵=E1 (DK_n, MK)

30 (3) 鍵計算部103

鍵計算部103は、記録装置100に割り当てられた装置番号「1」を予め記憶している。

鍵計算部103は、メディア鍵データ格納部102に記憶されているメディア鍵データMDATAを構成するn個の組から、予め記憶している装置番号

- 5 「1」を含む組を探して読み出し、読み出した組から装置番号「1」に対応する暗号化メディア鍵E1（DK__1、MK）を抽出する。

次に、鍵計算部103は、デバイス鍵格納部101からデバイス鍵DK__1を読み出し、読み出したデバイス鍵DK__1を用いて、抽出した暗号化メディア鍵E1（DK__1、MK）に復号アルゴリズムD1を施して、メディア鍵M

- 10 Kを生成する。

メディア鍵 $MK = D1(DK_1, (E1(DK_1, MK)))$

ここで、復号アルゴリズムD1は、暗号化アルゴリズムE1を施して生成された暗号文を復号するアルゴリズムであり、一例として、DESによるものである。また、D(A、B)は、鍵Aを用いて、暗号文Bに対して復号アルゴリズムDを施して得られた復号文を示している。

- 15

次に、鍵計算部103は、生成したメディア鍵MKを鍵計算部104へ出力する。

なお、図2において、記録装置100の各構成部を示す各ブロックは、接続線により他のブロックと接続されている。ただし、一部の接続線を省略している。ここで、各接続線は、信号や情報が伝達される経路を示している。また、鍵計算部103を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが描かれているものは、鍵計算部103へ鍵としての情報が伝達される経路を示している。他の構成要素を示すブロックについても同様である。また、他の図面についても同様である。

- 20

25 (4) 鍵計算部104

鍵計算部104は、鍵計算部103からメディア鍵MKを受け取り、ドライブ部111を介して、記録媒体120の固有番号記録領域121から媒体固有番号MIDを読み出す。

次に、鍵計算部104は、受け取ったメディア鍵MKと読み出した媒体固有番号MIDを、この順序で、結合して、結合値(MK || MID)を生成する。

- 30

ここで、「 $A || B$ 」は、データAとデータBとをこの順序でビット結合することを示す。次に、鍵計算部104は、生成した結合値($MK || MID$)にハッシュ関数SHA-1を施して、ハッシュ値 $H = SHA-1(MK || MID)$ を得、得られたハッシュ値Hを鍵暗号化鍵KEKとし、鍵暗号化鍵KEKを暗号化部105及び署名生成部110へ出力する。

ここで、 $SHA-1(A)$ は、情報Aに対してハッシュ関数SHA-1を施して得られたハッシュ値を示している。

なお、鍵計算部104は、ハッシュ関数SHA-1を施して得られたハッシュ値を鍵暗号化鍵KEKとしているが、これに限定されることはない。得られたハッシュ値の一部分を鍵暗号化鍵KEKとしてもよい。

また、ハッシュ関数SHA-1については、公知であるので、説明を省略する。なお、他のハッシュ関数を使用してもよい。

(5) 暗号化部105

暗号化部105は、コンテンツサーバ装置500から送受信部113を介して、コンテンツ鍵CKを受け取り、鍵計算部104から鍵暗号化鍵KEKを受け取る。

次に、暗号化部105は、受け取った鍵暗号化鍵KEKを用いて、受け取ったコンテンツ鍵CKに暗号化アルゴリズムE2を施して、暗号化コンテンツ鍵ECKを生成する。

20 暗号化コンテンツ鍵 $ECK = E2(KEK, CK)$

ここで、暗号化アルゴリズムE2は、一例として、DESによるものである。

次に、暗号化部105は、ドライブ部111を介して、記録媒体120上に鍵記録領域123を確保し、次に、生成した暗号化コンテンツ鍵ECKを、ドライブ部111を介して、記録媒体120の鍵記録領域123へ書き込む。

25 (6) 暗号化部106

暗号化部106は、コンテンツサーバ装置500から送受信部113を介して、コンテンツ鍵CK及びコンテンツCNTを受け取り、受け取ったコンテンツ鍵CKを用いて、受け取ったコンテンツCNTに暗号化アルゴリズムE3を施して暗号化コンテンツECNTを生成する。

30 暗号化コンテンツ $ECNT = E3(CK, CNT)$

ここで、暗号化アルゴリズムE3は、一例として、DESによるものである。

次に、暗号化部106は、ドライブ部111を介して、記録媒体120上にコンテンツ記録領域124を確保し、次に、生成した暗号化コンテンツENC Tを、ドライブ部111を介して、記録媒体120のコンテンツ記録領域124へ書き込む。

(7) 秘密鍵格納部107

秘密鍵格納部107は、外部の装置からアクセスできないように、記録装置100の秘密鍵SK__1を記憶している。秘密鍵SK__1は、公開鍵暗号方式によるものである。ここで、前記公開鍵暗号方式は、一例として、RSA (Rivest Shamir Adleman) 暗号方式である。

(8) 証明書格納部108

証明書格納部108は、公開鍵証明書PKCを記憶している。公開鍵証明書PKCは、証明書識別子ID__1、公開鍵PK__1及び署名データSig__1を含んで構成される。

証明書識別子ID__1は、公開鍵証明書PKCを一意に識別する識別情報である。公開鍵PK__1は、秘密鍵格納部107に記憶されている秘密鍵SK__1に対応する公開鍵である。また、署名データSig__1は、認証局CA (Certificate Authority) の秘密鍵SK__CAを用いて、証明書識別子ID__1及び公開鍵PK__1の結合値(ID__1 || PK__1)に対してデジタル署名Sigを施して生成されたものである。

署名データSig__1 = Sig (SK__CA, ID__1 || PK__1)

ここで、Sig (A, B) は、鍵Aを用いて、データBに対して、デジタル署名Sigを施して得られた署名データを示している。また、デジタル署名Sigの一例は、ハッシュ関数SHA-1を使ったRSAを用いるデジタル署名である。

(9) CRL格納部109

CRL格納部109は、第1の時点における無効化された公開鍵証明書を示す公開鍵証明書無効化リスト（以下、無効化リストCRLと呼ぶ。）を記録している。

無効化リストCRLは、1個以上の証明書識別子と、署名データSig ID

と、版数とを含んでいる。

各証明書識別子は、無効化された公開鍵証明書を識別する識別情報である。

- 署名データ $SigID$ は、認証局 CA の秘密鍵 SK_CA を用いて、無効化リスト CRL に含まれる全ての証明書識別子の結合値に対して（無効化リスト
- 5 CRL に 1 個の証明書識別子が含まれている場合には、前記 1 個の証明書識別子に対して）、デジタル署名 Sig を施して生成されたものである。

署名データ $SigID = Sig(SK_CA, \text{全ての証明書識別子の結合値})$

- 例えば、証明書識別子 ID_3 及び ID_4 により識別される公開鍵証明書が無効化されている場合には、無効化リスト CRL は、証明書識別子 ID_3 、
- 10 ID_4 、署名データ $SigID = Sig(SK_CA, (ID_3 || ID_4))$ 及び版数を含む。

版数は、無効化リスト CRL の世代を示す情報であり、無効化リスト CRL が前記第 1 の時点におけるものであることを示す。版数は、公開鍵証明書無効化リストの世代が新しいほど、大きい値をとる。

- 15 (10) 署名生成部 110

署名生成部 110 は、秘密鍵格納部 107 から秘密鍵 SK_1 を読み出し、 CRL 格納部 109 から無効化リスト CRL を読み出し、鍵計算部 104 から鍵暗号化鍵 KEK を受け取る。

- 次に、署名生成部 110 は、受け取った鍵暗号化鍵 KEK と読み出した無効
- 20 化リスト CRL とをこの順序で結合して結合値 $(KEK || CRL)$ を生成し、読み出した秘密鍵 SK_1 を用いて、生成した結合値 $(KEK || CRL)$ にデジタル署名 Sig を施して署名データ $SigCRL$ を生成する。

署名データ $SigCRL = Sig(SK_1, (KEK || CRL))$

- 次に、署名生成部 110 は、ドライブ部 111 を介して、記録媒体 120 上
- 25 に署名記録領域 125 を確保し、次に、生成した署名データ $SigCRL$ を、ドライブ部 111 を介して、記録媒体 120 の署名記録領域 125 へ書き込む。

(11) 制御部 112

制御部 112 は、送受信部 113 を介して、コンテンツサーバ装置 500 に対して、コンテンツの取得要求を送信する。

- 30 また、制御部 112 は、証明書格納部 108 から公開鍵証明書 PKC を読み

出し、ドライブ部111を介して、記録媒体120上に証明書記録領域127を確保し、次に、読み出した公開鍵証明書PKCをドライブ部111を介して、記録媒体120の証明書記録領域127へ書き込む。

また、制御部112は、メディア鍵データ格納部102からメディア鍵データMDATAを読み出し、ドライブ部111を介して、記録媒体120上にメディア鍵データ記録領域122を確保し、次に、読み出したメディア鍵データMDATAをドライブ部111を介して、記録媒体120のメディア鍵データ記録領域122へ書き込む。

また、制御部112は、CRL格納部109から無効化リストCRLを読み出し、ドライブ部111を介して、記録媒体120上にCRL記録領域126を確保し、次に、読み出した無効化リストCRLをドライブ部111を介して、記録媒体120のCRL記録領域126へ書き込む。

制御部112は、記録装置100の操作者の操作指示によりキーボード180から指示情報を受け取り、指示情報に従って動作する。また、記録装置100を構成する他の構成要素の動作を制御する。

(12) 送受信部113

送受信部113は、専用回線30を介して、コンテンツサーバ装置500と接続されており、コンテンツサーバ装置500と制御部112との間で情報の送受信を行う。また、制御部112の制御の基に、コンテンツサーバ装置500と暗号化部105との間で、及びコンテンツサーバ装置500と暗号化部106との間で、情報の送受信を行う。

(13) ドライブ部111

ドライブ部111は、制御部112の制御の基に、記録媒体120の固有番号記録領域121から媒体固有番号MIDを読み出し、読み出した媒体固有番号MIDを鍵計算部104へ出力する。

また、ドライブ部111は、制御部112の制御の基に、暗号化部105、暗号化部106、署名生成部110から各情報を受け取り、受け取った情報を書き込むための各領域を記録媒体120上に確保し、確保した領域に前記情報を書き込む。

また、ドライブ部111は、制御部112から情報を受け取り、受け取った

情報を書き込むための各領域を記録媒体120上に確保し、確保した領域に前記情報を書き込む。

(14) キーボード180及びモニタ190

5 キーボード180は、記録装置100の操作者の操作指示を受け付け、受け付けた操作指示に対応する指示情報を制御部112へ出力する。

モニタ190は、制御部112の制御により様々な情報を表示する。

1. 4 記録媒体120

記録媒体120は、光ディスクメディアであり、図3に示すように、固有番号記録領域121と、一般領域129とから構成されている。

10 固有番号記録領域121には、記録媒体120を識別する固有の番号である媒体固有番号MIDが予め記録されている。固有番号記録領域121は、他の情報の書き込みや記録されている媒体固有番号MIDの書き換えができない書換不可領域である。媒体固有番号MIDは、一例として、16進数8桁で表現されており、「0x00000006」である。なお、本明細書において、「0x」は、以降の表示が16進数によるものであることを示している。

一般領域129は、他の情報の書き込みが可能な領域であり、当初、一般領域129には、何らの情報も書き込まれていない。

記録装置100の上述した動作の終了後において、一般領域129には、図3に示すように、メディア鍵データ記録領域122、鍵記録領域123、コンテンツ記録領域124、署名記録領域125、CRL記録領域126及び証明書記録領域127が確保される。

25 上述したように、第1の実施の形態では、記録装置100及び再生装置200a、200b、200c、200d、200e、・・・の台数の合計がn台であり、これらの装置のうち、再生装置200b及び再生装置200cが無効化されており、n台の装置はそれぞれ固有のデバイス鍵を1つだけ保有している、と仮定している。このような仮定に基づいて、記録媒体120の一般領域129に含まれている各領域には、具体例としての各種データが記録されている。

(メディア鍵データ記録領域122)

30 メディア鍵データ記録領域122には、メディア鍵データMDATAが記録

されている。メディア鍵データMDATAは、n個の組から構成され、各組は、暗号化メディア鍵及び装置番号を含む。

装置番号は、装置を識別する識別情報である。

- 5 暗号化メディア鍵は、対応する装置番号「m」により示される装置mに割り当てられたデバイス鍵DK__mを用いて、メディア鍵MK又は値「0」に暗号化アルゴリズムE1を施して生成されたものである。ここで、装置mが無効化されている場合には、値「0」を用いる。また、装置mが無効化されていない場合には、メディア鍵MKを用いる。

暗号化メディア鍵 = E1 (DK__m, MK) 又は

- 10 暗号化メディア鍵 = E1 (DK__m, 0)

(鍵記録領域123)

鍵記録領域123には、暗号化コンテンツ鍵ECKが記録されている。暗号化コンテンツ鍵ECKは、鍵暗号化鍵KEKを用いて、コンテンツ鍵CKに暗号化アルゴリズムE2を施して生成されたものである。

- 15 暗号化コンテンツ鍵ECK = E2 (KEK, CK)

ここで、鍵暗号化鍵KEKは、メディア鍵MKと媒体固有番号MIDを結合した値を入力値として、ハッシュ関数の出力値を利用して算出される鍵である。

鍵暗号化鍵KEK = SHA-1 (MK || MID)

(コンテンツ記録領域124)

- 20 コンテンツ記録領域124には、暗号化コンテンツECNTが記録されている。暗号化コンテンツECNTは、コンテンツ鍵CKを用いて、コンテンツに暗号化アルゴリズムE3を施して生成されたものである。

暗号化コンテンツECNT = E3 (CK, CNT)

(署名記録領域125)

- 25 署名記録領域125には、署名データSigCRLが記録されている。

署名データSigCRLは、秘密鍵SK__1を用いて、鍵暗号化鍵KEKと無効化リストCRLとの結合値(KEK || CRL)にデジタル署名Sigを施して生成されたものである。

署名データSigCRL = Sig (SK__1, (KEK || CRL))

- 30 (CRL記録領域126)

CRL記録領域126には、無効化リストCRLが記録されており、無効化リストCRLには、無効化すべき証明書のIDが記載されている。無効化リストCRLは、一例として、証明書識別子ID__3、ID__4、署名データSigID及び版数を含んでいる。

- 5 証明書識別子ID__3、ID__4は、無効化された公開鍵証明書を識別する識別情報である。

署名データSigIDは、認証局CAの秘密鍵SK_CAを用いて、無効化リストCRLに含まれる全ての証明書識別子の結合値に対して（無効化リストCRLに1個の証明書識別子が含まれている場合には、前記1個の証明書識別子に対して）、デジタル署名Sigを施して生成されたものである。

- 10

署名データSigID=Sig(SK_CA、全ての証明書識別子の結合値)

認証局CAによる署名データが含まれているのは、無効化リストCRLの正当性を保証するためである。

版数は、無効化リストCRLの世代を示す情報である。

- 15 なお、CRLのフォーマットは公知のものであってもよいし、また、あるシステムに特化したフォーマットであってもよい。

（証明書記録領域127）

証明書記録領域127には、公開鍵証明書PKCが記録されている。公開鍵証明書PKCは、証明書識別子ID__1、公開鍵PK__1及び署名データSig__1を含んでいる。

- 20

証明書識別子ID__1は、公開鍵証明書PKCを識別する識別情報である。

公開鍵PK__1は、公開鍵暗号方式によるものであり、秘密鍵SK__1に対応している。

署名データSig__1は、認証局CAの秘密鍵SK_CAを用いて、証明書識別子ID__1及び公開鍵PK__1の結合値(ID__1 || PK__1)に対してデジタル署名Sigを施して生成されたものである。

- 25

署名データSig__1=Sig(SK_CA、ID__1 || PK__1)

なお、認証局CAによる署名データが含まれているのは、公開鍵証明書の正当性を保証するためである。

- 30 また、公開鍵証明書のフォーマットは公知のものであってもよいし、またあ

るシステムに特化したフォーマットであってもよい。

1. 5 再生装置200

再生装置200a、200b、200c、・・・は、同様の構成を有しているので、ここでは、再生装置200として説明する。

- 5 再生装置200は、図4に示すように、デバイス鍵格納部201、鍵計算部202、鍵計算部203、復号部204、復号部205、CA公開鍵格納部206、証明書検証部207、CRL格納部208、CRL検証部209、CRL比較更新部210、証明書判定部211、署名検証部212、スイッチ213、再生部214、制御部215、入力部216、表示部217及びドライブ部218から構成されている。

- 再生装置200は、具体的には、コンテンツサーバ装置500と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、再生装置200は、その機能を達成する。

(1) デバイス鍵格納部201

- デバイス鍵格納部201は、外部の装置からアクセスできないように、デバイス鍵DK__xを秘密に記憶している。デバイス鍵DK__xは、再生装置200に固有の鍵である。

- なお、デバイス鍵格納部201が記憶しているデバイス鍵DK__xは、再生装置200a、200b、200c、200d、200e、・・・により異なる。再生装置200a、200b、200c、200d、200e、・・・の各デバイス鍵格納部201は、それぞれ、デバイス鍵DK__2、DK__3、DK__4、DK__5、DK__6、・・・を記憶している。

(2) 鍵計算部202

- 鍵計算部202は、再生装置200に割り当てられた装置番号「x」を予め記憶している。なお、鍵計算部202が記憶している装置番号「x」は、再生装置200a、200b、200c、200d、200e、・・・により異なる。再生装置200a、200b、200c、200d、200e、・・・の

各鍵計算部202は、それぞれ、装置番号「2」、「3」、「4」、「5」、「6」・・・を記憶している。

鍵計算部202は、記録媒体120のメディア鍵データ記録領域122から、ドライブ部218を介して、メディア鍵データMDATAを構成するn個の組を順に読み出し、読み出した組の中から、記憶している装置番号「x」を含む組を探す。装置番号「x」を含む組を発見すると、発見した組から装置番号「x」に対応する暗号化メディア鍵E1 (DK_x, y) を抽出する。ここで、再生装置200が、再生装置200b又は200cである場合には、yは、値「0」である。また、再生装置200が、再生装置200b及び200cを除く他の再生装置である場合には、yは、メディア鍵MKである。

次に、鍵計算部202は、デバイス鍵格納部201からデバイス鍵DK_xを読み出し、読み出したデバイス鍵DK_xを用いて、抽出した暗号化メディア鍵E1 (DK_x, y) に復号アルゴリズムD1を施して、復号メディア鍵yを生成する。

15 復号メディア鍵 $y = D1 (DK_x, (E1 (DK_x, y)))$

ここで、復号メディア鍵yは、メディア鍵MK及び値「0」のいずれかである。

次に、鍵計算部202は、生成した復号メディア鍵yを鍵計算部203へ出力する。

20 (3) 鍵計算部203

鍵計算部203は、鍵計算部104と同様に動作する。

鍵計算部203は、鍵計算部202から復号メディア鍵yを受け取り、ドライブ部218を介して、記録媒体120の固有番号記録領域121から媒体固有番号MIDを読み出す。

25 次に、鍵計算部203は、受け取った復号メディア鍵yと読み出した媒体固有番号MIDを、この順序で、結合して、結合値 $(y || MID)$ を生成する。次に、鍵計算部203は、生成した結合値 $(y || MID)$ にハッシュ関数SHA-1を施して、ハッシュ値 $H' = SHA-1 (y || MID)$ を得、得られたハッシュ値H' を鍵復号鍵KDKとし、鍵復号鍵KDKを復号部204及び署名検証部212へ出力する。

なお、上述したように、鍵計算部104が、得られたハッシュ値の一部を鍵暗号化鍵KEKとする場合には、鍵計算部203も得られたハッシュ値の前記一部分と同じ部分を鍵復号鍵KDKとする。

(4) 復号部204

5 復号部204は、記録媒体120の鍵記録領域123から、ドライブ部218を介して、暗号化コンテンツ鍵ECKを読み出し、鍵計算部203から鍵復号鍵KDKを受け取る。

次に、復号部204は、受け取った鍵復号鍵KDKを用いて、読み出した暗号化コンテンツ鍵ECKに復号アルゴリズムD2を施して、復号コンテンツ鍵DCKを生成する。

復号コンテンツ鍵 $DCK = D2(KDK, ECK)$

ここで、復号アルゴリズムD2は、暗号化アルゴリズムE2を施して生成された暗号文を復号するアルゴリズムであり、一例として、DESによるものである。

15 次に、復号部204は、生成した復号コンテンツ鍵DCKを復号部205へ出力する。

(5) 復号部205

復号部205は、記録媒体120のコンテンツ記録領域124から、ドライブ部218を介して、暗号化コンテンツECNTを読み出し、復号部204から復号コンテンツ鍵DCKを受け取る。

次に、復号部205は、受け取った復号コンテンツ鍵DCKを用いて、読み出した暗号化コンテンツECNTに復号アルゴリズムD3を施して復号コンテンツDCNTを生成する。

復号コンテンツ $DCNT = D3(DCK, ECNT)$

25 ここで、復号アルゴリズムD3は、暗号化アルゴリズムE3を施して生成された暗号文を復号するアルゴリズムであり、一例として、DESによるものである。

次に、復号部205は、生成した復号コンテンツDCNTをスイッチ213へ出力する。

30 (6) CA公開鍵格納部206

CA公開鍵格納部206は、認証局CAの公開鍵PK_CAを予め記憶している。

(7) 証明書検証部207

5 証明書検証部207は、CA公開鍵格納部206から公開鍵PK_CAを読み出し、記録媒体120の証明書記録領域127から、ドライブ部218を介して、公開鍵証明書PKCを読み出す。

次に、証明書検証部207は、読み出した公開鍵証明書PKCから、証明書識別子ID_1、公開鍵PK_1及び署名データSig_1を抽出し、抽出した証明書識別子ID_1及び公開鍵PK_1をこの順序で結合して結合値(ID_1 || PK_1)を生成する。

次に、証明書検証部207は、読み出した公開鍵PK_CAを用いて、抽出した署名データSig_1及び生成した結合値(ID_1 || PK_1)に、署名検証アルゴリズムVrfyを施して、検証結果RSL2を得る。検証結果RSL2は、検証成功及び検証失敗のいずれかを示す情報である。

15 ここで、署名検証アルゴリズムVrfyは、デジタル署名Sigにより生成された署名データを検証するアルゴリズムである。

次に、証明書検証部207は、検証結果RSL2をスイッチ213へ出力する。

(8) CRL格納部208

20 CRL格納部208は、第2の時点における無効化された公開鍵証明書を示す公開鍵証明書無効化リスト（以下、蓄積無効化リストCRL_STと呼ぶ。）を記録している。

蓄積無効化リストCRL_STは、第1の時点における無効化された公開鍵証明書を示すリストである無効化リストCRLと同様に、1個以上の証明書識別子と、署名データSigIDと、版数とを含んでいる。

証明書識別子及び署名データSigIDについては、上述した通りである。

版数は、蓄積無効化リストCRL_STの世代を示す情報であり、蓄積無効化リストCRL_STが前記第2の時点におけるものであることを示す。版数は、公開鍵証明書無効化リストの世代が新しいほど、大きい値をとる。

30 (9) CRL検証部209

CRL検証部209は、CA公開鍵格納部206から公開鍵PK_CAを読み出し、記録媒体120のCRL記録領域126から、ドライブ部218を介して、無効化リストCRLを読み出す。

次に、CRL検証部209は、読み出した無効化リストCRLから1個以上の証明書識別子と署名データSigIDとを抽出する。ここで、複数の証明書識別子が抽出された場合には、これらが無効化リストCRL内に配置されている順序で結合して結合値を生成する。また、1個の証明書識別子のみが抽出された場合には、抽出された1個の証明書識別子を前記結合値とする。

次に、CRL検証部209は、読み出した公開鍵PK_CAを用いて、抽出した署名データSigIDと生成した前記結合値とに、署名検証アルゴリズムVrfyを施して、検証結果RSL3を得る。検証結果RSL3は、検証成功及び検証失敗のいずれかである。

得られた検証結果RSL3が検証成功を示す場合には、CRL検証部209は、読み出した無効化リストCRLを署名検証部212及びCRL比較更新部210へ出力する。

(10) CRL比較更新部210

CRL比較更新部210は、CRL検証部209から無効化リストCRLを受け取る。

無効化リストCRLを受け取った場合に、CRL比較更新部210は、受け取った無効化リストCRLから版数を抽出し、CRL格納部208から蓄積無効化リストCRL_STを読み出し、読み出した蓄積無効化リストCRL_STから版数を抽出する。次に、無効化リストCRLから抽出した版数が、蓄積無効化リストCRL_STから抽出した版数より大きい、否かを判断する。

無効化リストCRLから抽出した版数が、蓄積無効化リストCRL_STから抽出した版数より大きいと判断した場合に、CRL比較更新部210は、無効化リストCRLの世代は、蓄積無効化リストCRL_STの世代より新しいとみなし、無効化リストCRLを、蓄積無効化リストCRL_STとして、CRL格納部208に上書きする。

無効化リストCRLから抽出した版数が、蓄積無効化リストCRL_STから抽出した版数より小さいか又は等しいと判断した場合に、無効化リストCR

Lの世代は、蓄積無効化リストCRL__STの世代より古いか又は同じとみなされ、上記の上書きは行われない。

(11) 証明書判定部211

証明書判定部211は、CRL格納部208から蓄積無効化リストCRL__STを読み出す。ここで、CRL格納部208に記憶されている蓄積無効化リストCRL__STは、CRL比較更新部210により、最新のものに更新されている。また、証明書判定部211は、記録媒体120の証明書記録領域127から、ドライブ部218を介して、公開鍵証明書PKCを読み出す。

次に、証明書判定部211は、読み出した公開鍵証明書PKCから証明書識別子ID__1を抽出し、抽出した証明書識別子ID__1が、蓄積無効化リストCRL__STに含まれているか否かを判断する。次に、判断結果JDGをスイッチ213へ出力する。ここで、判断結果JDGは、証明書識別子ID__1が蓄積無効化リストCRL__STに含まれているか否かを示す情報である。

(12) 署名検証部212

署名検証部212は、鍵計算部203から鍵復号鍵KDKを受け取る。また、記録媒体120の署名記録領域125から、ドライブ部218を介して、署名データSigCRLを読み出し、記録媒体120の証明書記録領域127から、ドライブ部218を介して、公開鍵証明書PKCを読み出す。また、CRL検証部209から無効化リストCRLを受け取る。

次に、署名検証部212は、読み出した公開鍵証明書PKCから公開鍵PK__1を抽出し、受け取った鍵復号鍵KDKと受け取った無効化リストCRLを結合して結合値(KDK||CRL)を生成し、抽出した公開鍵PK__1を用いて、読み出した署名データSigCRL及び生成した結合値(KDK||CRL)に署名検証アルゴリズムVrfyを施して、検証結果RSL1を得る。検証結果RSL1は、検証成功及び検証失敗のいずれかを示す情報である。

次に、署名検証部212は、検証結果RSL1をスイッチ213へ出力する。

(13) スイッチ213

スイッチ213は、復号部205から復号コンテンツDCNTを受け取る。また、証明書判定部211から判断結果JDGを受け取り、証明書検証部207から検証結果RSL2を受け取り、署名検証部212から検証結果RSL1

を受け取る。

受け取った検証結果RSL1が検証成功を示し、かつ受け取った検証結果RSL2が検証成功を示し、かつ受け取った判断結果JDGが、証明書識別子ID_1が蓄積無効化リストCRL_STに含まれていないことを示す場合に限り、スイッチ213は、受け取った復号コンテンツDCNTを再生部214へ出力する。

受け取った検証結果RSL1が検証失敗を示し、又は受け取った検証結果RSL2が検証失敗を示し、又は受け取った判断結果JDGが、証明書識別子ID_1が蓄積無効化リストCRL_STに含まれていることを示す場合に、スイッチ213は、受け取った復号コンテンツDCNTを再生部214へ出力しない。

(14) 再生部214

再生部214は、スイッチ213から復号コンテンツDCNTを受け取り、受け取った復号コンテンツDCNTから映像情報及び音声情報を生成し、生成した映像情報及び音声情報をアナログの映像信号及び音声信号に変換し、アナログの映像信号及び音声信号をモニタ290へ出力する。

(15) 制御部215、入力部216、表示部217、ドライブ部218、モニタ290及びリモコン280

制御部215は、再生装置200を構成する各構成要素の動作を制御する。

リモコン280は、各種のボタンを備え、操作者の前記ボタンの操作に応じた操作指示情報を生成し、生成した操作指示情報を赤外線に乗せて出力する。

入力部216は、リモコン280から、操作指示情報が乗せられた赤外線を受け取り、受け取った赤外線から操作指示情報を抽出し、抽出した操作指示情報を制御部215へ出力する。

表示部217は、制御部215の制御の基に、様々な情報を表示する。

ドライブ部218は、記録媒体120からの情報の読み出しを行う。

モニタ290は、CRT及びスピーカを備え、再生部214からアナログの映像信号及び音声信号を受信し、映像信号に基づいて映像を表示し、音声信号に基づいて音声を出力する。

1. 6 コンテンツ供給システム10の動作

コンテンツ供給システム10の動作について、特に、記録装置100による記録媒体120へのデータの書き込みの動作及び再生装置200による記録媒体120に記録されているデータの再生の動作について、説明する。

(1) 記録装置100による書き込みの動作

- 5 記録装置100による記録媒体120へのデータの書き込みの動作について、図5に示すフローチャートを用いて説明する。

鍵計算部103は、デバイス鍵格納部101及びメディア鍵データ格納部102から、それぞれ、デバイス鍵DK__1及びメディア鍵データMDATAを読み出し（ステップS301）、次に、読み出したデバイス鍵DK__1及びメディア鍵データMDATAを用いて、メディア鍵MKを生成する（ステップS302）。

10

次に、鍵計算部104は、記録媒体120の固有番号記録領域121から媒体固有番号MIDを読み出し（ステップS303）、生成されたメディア鍵MIDと読み出した媒体固有番号MIDを用いて、鍵暗号化鍵KEKを算出する（ステップS304）。

15

次に、暗号化部105は、算出された鍵暗号化鍵KEKを用いて、コンテンツサーバ装置500から取得したコンテンツ鍵CKを暗号化して、暗号化コンテンツ鍵ECKを生成する（ステップS305）。

次に、暗号化部106は、コンテンツサーバ装置500から取得したコンテンツ鍵CKを用いて、コンテンツサーバ装置500から取得したコンテンツCNTを暗号化して暗号化コンテンツECNTを生成する（ステップS306）。

20

次に、署名生成部110は、秘密鍵格納部107から秘密鍵SK__1を読み出し（ステップS307）、読み出した秘密鍵SK__1を用いて、鍵暗号化鍵KEK及び無効化リストCRLに対する署名データSigCRLを生成する（ステップS308）。

25

次に、記録装置100は、メディア鍵データMDATA、暗号化コンテンツ鍵ECK、暗号化コンテンツECNT、署名データSigCRL、無効化リストCRL及び公開鍵証明書PKCを、ドライブ部111を介して、記録媒体120に記録する（ステップS309）。

- 30 (2) 再生装置200による再生の動作

再生装置200による記録媒体120に記録されているデータの再生の動作について、図6～図7に示すフローチャートを用いて説明する。

- 再生装置200は、記録媒体120から、メディア鍵データMDATA、媒体固有番号MID、暗号化コンテンツ鍵ECK、暗号化コンテンツECNT、署名データSigCRL、無効化リストCRL及び公開鍵証明書PKCを読み出す（ステップS401）。

次に、鍵計算部202は、デバイス鍵格納部201からデバイス鍵DK_xを読み出し（ステップS402）、読み出したメディア鍵データMDATA及びデバイス鍵DK_xを用いて、復号メディア鍵_yを得る（ステップS403）。

- 次に、鍵計算部203は、読み出した媒体固有番号MID及び得られた復号メディア鍵_yから鍵復号鍵KDKを算出する（ステップS404）。

次に、復号部204は、算出された鍵復号鍵KDKを用いて、読み出した暗号化コンテンツ鍵ECKを復号して復号コンテンツ鍵DCKを得る（ステップS405）。

- 次に、復号部205は、読み出した暗号化コンテンツECNTを、得られた復号コンテンツ鍵DCKを用いて、復号して、復号コンテンツDCNTを得る（ステップS406）。

- 次に、証明書検証部207は、CA公開鍵格納部206から認証局CAの公開鍵PK_{CA}を読み出し（ステップS407）、読み出した認証局CAの公開鍵PK_{CA}を用いて、読み出した公開鍵証明書PKCの正当性を検証する（ステップS408）。

- 公開鍵証明書PKCの正当性の検証に失敗した場合には（ステップS409）、ステップS422へ制御が移る。公開鍵証明書PKCの正当性の検証に成功した場合には（ステップS409）、CRL検証部209は、認証局CAの公開鍵PK_{CA}を用いて、読み出した無効化リストCRLの正当性を検証する（ステップS410）。

- 無効化リストCRLの正当性の検証に失敗した場合には（ステップS411）、ステップS422へ制御が移る。無効化リストCRLの正当性の検証に成功した場合には（ステップS411）、CRL比較更新部210は、CRL格納部208から蓄積無効化リストCRL_{ST}を読み出し（ステップS412）、

記録媒体120から読み出した無効化リストCRLと、CRL格納部208から読み出した蓄積無効化リストCRL__STとの新旧を比較する（ステップS413）。

5 CRL比較更新部210は、上記の比較の結果、無効化リストCRLの方が、蓄積無効化リストCRL__STより新しいと判断される場合に（ステップS414）、新しいと判断した無効化リストCRLを蓄積無効化リストCRL__STとして、CRL格納部208に上書きする（ステップS415）。無効化リストCRLの方が、蓄積無効化リストCRL__STより古いと判断される場合（ステップS414）、ステップS416へ制御が移る。

10 次に、証明書判定部211は、CRL格納部208から蓄積無効化リストCRL__STを読み出し（ステップS416）、読み出した公開鍵証明書PKCから抽出した証明書識別子ID__1が、蓄積無効化リストCRL__STに含まれているか否かを判断することにより、読み出した蓄積無効化リストCRL__STに公開鍵証明書PKCが登録されているか否かを判定する（ステップS417）。

15 登録されていると判定された場合（ステップS418）、ステップS422へ制御が移る。登録されていないと判定された場合（ステップS418）、署名検証部212は、鍵復号鍵KDK、公開鍵証明書PKC及び無効化リストCRLを用いて、署名データSigCRLの正当性を検証する（ステップS419）。

20 署名データSigCRLの正当性の検証に失敗した場合（ステップS420）、スイッチ213は、開かれ、コンテンツは再生されず（ステップS422）、再生装置200の再生動作が終了する。

25 一方、署名データSigCRLの正当性の検証に成功した場合（ステップS420）、スイッチ213は、閉じられ、復号コンテンツDCNTを再生部214へ出力し、再生部214は、復号コンテンツDCNTを再生し（ステップS421）、再生装置200の再生動作が終了する。

1. 7 その他の変形例

30 （1）第1の実施の形態では、記録媒体を介して、無効化リストCRLを伝播する仕組みを実現するために、記録装置が、無効化リストCRLを署名対象

として署名データ $SigCRL$ を生成し、生成した署名データ $SigCRL$ を記録媒体に書き込むとしているが、本発明は、この構成に限定されるものではない。

例えば、記録装置は、無効化リスト CRL のハッシュ値を算出して、そのハッシュ値に対して署名データを生成するとしてもよい。

署名データ = $Sig(SK_1, HASH(CRL))$

ここで、 $HASH(A)$ は、データ A に対してハッシュ関数 $HASH$ を施して得られたハッシュ値である。

また、記録装置は、無効化リスト CRL のハッシュ値を算出して、そのハッシュ値とメディア鍵 MK を XOR (排他的論理和) 演算し、その演算結果に対して署名データを生成するとしてもよい。

署名データ = $Sig(SK_1, (HASH(CRL)) XOR (MK))$

このように、記録装置は、無効化リスト CRL 及びコンテンツに対して署名データを生成したり、無効化リスト CRL 及び各種鍵データに対して署名データを生成したりし、生成した署名データを記録媒体に書き込むことにより、記録媒体上の無効化リスト CRL の改ざんや削除を防止することができる。

また、これらの場合に、再生装置は、それぞれ、対応するデータを用いて、署名検証を行う。

(2) 第1の実施の形態では、外部から取得する無効化リスト CRL 及び内部に記憶している無効化リスト CRL の新旧を比較する際に、バージョン番号を比較するとしているが、本発明は、この構成に限定されるものではない。

例えば、無効化リスト CRL が更新されるにつれて、無効化リスト CRL のサイズが単調に増加すると仮定できれば、 CRL のサイズが大きい方を新しいと判断してもよい。

同様に、無効化リスト CRL が更新されるにつれて、無効化される装置の数が単調に増加すると仮定できれば、無効化する装置の台数の比較により、無効化台数が多い方を新しいと判断してもよい。

以上のように、 CRL から新旧比較できる情報を得ることができる構成であれば、如何なる構成であってもよい。

(3) 別の記録媒体を介して、メディア鍵データの最新版が、記録装置に対

して、伝播する構成であってもよい。

前記別の記録媒体には、最新版のメディア鍵データが記録されている。

記録装置は、内部に予めメディア鍵データを保有している。メディア鍵データが記録されている前記別の記録媒体が装着されると、記録装置は、自身が保有しているメディア鍵データと、記録媒体に記録されているメディア鍵データとの新旧を比較し、自身が保有するメディア鍵データよりも、記録媒体に記録されているメディア鍵データの方が、新しければ、自ら保有しているメディア鍵データに代えて、記録媒体に記録されているメディア鍵データを内部に書き込む。

10 ここで、各メディア鍵データには、その世代を示すバージョン番号が付与されており、記録装置は、各バージョン番号を用いて、各メディア鍵データの新旧を比較する。

また、メディア鍵データから算出されるメディア鍵の一部はバージョン番号であり、残りの部分は、乱数を用いて生成されるときともよい。記録装置は、
15 各メディア鍵データからメディア鍵の一部のバージョン番号を抽出し、抽出した各バージョン番号を用いて、各メディア鍵データの新旧を比較する。

また、メディア鍵データにおいて無効化されている装置の台数、つまり、メディア鍵MKに代えて値「0」が暗号化の対象となっている暗号化メディア鍵の数は、メディア鍵データの更新につれて、単調に増加すると仮定し、記録装置は、メディア鍵データに含まれている無効化されている装置の台数を用いて、
20 各メディア鍵データの新旧を比較するときともよい。

また、各メディア鍵データには、当該メディア鍵データが生成された時刻情報（年月日時分秒）が付与されており、記録装置は、各時刻情報を用いて、各メディア鍵データの新旧を比較するときともよい。

25 以上のように、メディア鍵データの新旧を正しく比較できる構成であれば、如何なる構成であってもよい。

また、各メディア鍵データには、改ざん防止のための認証局CAの署名が付与されているときともよい。記録装置は、署名を検証することにより、メディア鍵データの正当性を確認する。

30 （４）メディア鍵データ及び暗号化コンテンツなどが予め記録されている記

録媒体に対して、さらに、別の暗号化コンテンツを追加して書き込む場合に、記録装置は、自身が保有するメディア鍵データに基づいて、又は前記記録媒体に記録されているメディア鍵データに基づいて、外部（例えば、コンテンツサーバ装置）から取得したコンテンツを暗号化して、別の暗号化コンテンツを生成し、生成した別の暗号化コンテンツを前記記録媒体に書き込むとしてもよい。

この場合、前記記録媒体上には、複数のメディア鍵データ、複数の公開鍵証明書、複数の無効化リストCRLが存在する場合がある。

また、記録装置は、前記記録媒体上のメディア鍵データと、記録装置が保有しているメディア鍵データとの新旧を比較し、記録装置が保有しているメディア鍵データの方が新しければ、前記記録媒体に記録されている暗号化コンテンツを復号して、復号コンテンツを生成し、生成した復号コンテンツを自身が保有する新しいメディア鍵に基づいて暗号化して、再暗号化コンテンツを生成し、生成した再暗号化コンテンツを前記記録媒体に書き込むとしてもよい。このとき、前記記録媒体に記録されている暗号化コンテンツを削除するとしてもよい。

（５）第１の実施の形態では、鍵暗号化鍵KEKに対して、デジタル署名を施して署名データを生成するとしているが、本発明はこの構成に限定されるものではない。

例えば、コンテンツCNT全体のハッシュ値に対して、デジタル署名を施して署名データを生成するとしてもよい。

署名データ＝Sig（SK₁、（HASH（CNT））

即ち、署名は、コンテンツを記録した記録装置の正当性の確認が目的であるため、署名の対象となるデータは、コンテンツに関連する情報や暗号化の際に用いる鍵に関連する情報であれば、如何なる情報であってもよい。

（６）第１の実施の形態では、記録装置１００は、図２に示すように、デバイス鍵格納部１０１、メディア鍵データ格納部１０２、鍵計算部１０３、鍵計算部１０４、暗号化部１０５、暗号化部１０６、秘密鍵格納部１０７、証明書格納部１０８、CRL格納部１０９、署名生成部１１０、ドライブ部１１１、制御部１１２及び送受信部１１３から構成される一体の装置であるとしているが、本発明は、この構成には限定されない。

例えば、デバイス鍵格納部１０１、メディア鍵データ格納部１０２、鍵計算

部 103、鍵計算部 104、暗号化部 105、暗号化部 106、秘密鍵格納部 107、証明書格納部 108、CRL 格納部 109、署名生成部 110、ドライブ部 111 及び制御部 112 の一部が一体となったドライブ装置から構成され、制御部 112 の他の一部及び送受信部 113 が一体となった処理装置から
5 構成されているとしてもよい。この構成では、記録媒体に対するデータの読出／書込及び暗号処理を行うドライブ装置と、他の処理を行う処理装置とに分離している。

また、デバイス鍵格納部 101、メディア鍵データ格納部 102、秘密鍵格納部 107、証明書格納部 108 及び CRL 格納部 109 は、外部の記憶装置
10 の記憶領域上に構成されているとしてもよい。ここで、前記外部の記憶装置の一例は、可搬型のセキュアなメモリカードである。

また、第 1 の実施の形態では、再生装置 200 は、図 4 に示すように、デバイス鍵格納部 201、鍵計算部 202、鍵計算部 203、復号部 204、復号部 205、CA 公開鍵格納部 206、証明書検証部 207、CRL 格納部 20
15 8、CRL 検証部 209、CRL 比較更新部 210、証明書判定部 211、署名検証部 212、スイッチ 213、再生部 214、制御部 215、入力部 216、表示部 217 及びドライブ部 218 から構成される一体の装置であるとしているが、本発明は、この構成には限定されない。

デバイス鍵格納部 201、鍵計算部 202、鍵計算部 203、復号部 204、
20 復号部 205、CA 公開鍵格納部 206、証明書検証部 207、CRL 格納部 208、CRL 検証部 209、CRL 比較更新部 210、証明書判定部 211、署名検証部 212、スイッチ 213 及びドライブ部 218 から構成される一体となったドライブ装置から構成され、再生部 214、制御部 215、入力部 216 及び表示部 217 から構成される一体となった処理装置から構成されているとしてもよい。この構成では、記録媒体に対するデータの読出／書込及び暗
25 号処理を行うドライブ装置と、他の処理を行う処理装置とに分離している。

また、デバイス鍵格納部 201、CA 公開鍵格納部 206 及び CRL 格納部 208 は、外部の記憶装置の記憶領域上に構成されているとしてもよい。ここで、前記外部の記憶装置の一例は、可搬型のセキュアなメモリカードである。

30 以上のように、記録装置及び再生装置は、それぞれ、一体の装置ではなく、

データ読出／書込装置及び処理装置の別々の構成であってもよい。この場合、データ読出／書込装置で暗号処理を行としてもよいし、処理装置で暗号処理を行うとしてもよい。

(7) 第1の実施の形態では、メディア鍵データMDATA、暗号化コンテンツ鍵ECK、暗号化コンテンツECNT、署名データSigCRL、無効化リストCRL及び公開鍵証明書PKCを全て同一の記録媒体に記録するとしているが、本発明は、この構成に限定されるものではない。

例えば、記録装置100は、署名データSigCRL、無効化リストCRL、公開鍵証明書PKCなどのデータの一部を、記録媒体120とは別の記録媒体に記録し、記録媒体120及びこの別の記録媒体が配布されとしてもよい。

また、記録装置100は、インターネットを代表とするネットワークに接続されており、これらのデータの一部を、ネットワークを介して配布するとしてもよい。再生装置200も、ネットワークに接続されており、記録装置100から、ネットワークを介して、これらのデータの一部を取得する。

15 以上のように、メディア鍵データMDATA、暗号化コンテンツ鍵ECK、暗号化コンテンツECNT、署名データSigCRL、無効化リストCRL及び公開鍵証明書PKCが、1個以上の記録媒体に記録されて配布され、又は、1個以上の記録媒体に記録されかつネットワークを介して配布されとしてもよい。

20 (8) 第1の実施の形態では、デバイス鍵に基づいて、コンテンツを暗号化し、また暗号化コンテンツを復号しているが、本発明は、この構成に限定されるものではない。

例えば、記録装置及び再生装置が利用条件を取得しており、その利用条件に基づいて記録及び再生を制御する構成であってもよい。ここで、利用条件とは、
25 コンテンツに付随する管理情報であり、例えば、コンテンツの記録及び再生を許可する日付、時間、又は回数である。

(9) 第1の実施の形態では、再生装置がCRL格納部から無効化リストCRLを読み出して新旧比較を行い、新しい無効化リストCRLをCRL格納部に格納し、公開鍵証明書の登録有無の確認時に再度、無効化リストCRLを読み出すとしているが、本発明は、この構成に限定されるものではない。

例えば、再生装置は、無効化リストCRLの新旧比較を行うことなく、また、新しいと判断した無効化リストCRLをCRL格納部に格納することなく、公開鍵証明書の無効化リストCRLでの登録の有無を判定した後に、記録媒体120から読み出した無効化リストCRLをCRL格納部へ格納するとしてもよい。

また、署名検証、CRL検証、公開鍵証明書判定の順序も、第1の実施の形態に記載の如く限定されず、再生装置は、種々の順序により、署名検証、CRL検証、公開鍵証明書判定を行い、コンテンツの再生を制御するとしてもよい。

(10) 記録装置及び再生装置が電子透かしを生成して埋め込む電子透かし処理部を備える構成であってもよい。

例えば、記録装置がその装置を特定する装置IDを記憶しており、コンテンツの記録媒体への記録時に、コンテンツに対して、その装置IDを電子透かしとして埋め込むとしてもよい。

このとき、装置IDが電子透かしとして埋め込まれたコンテンツが不正流出した場合に、コンテンツから、埋め込まれた装置IDを抽出することにより、そのコンテンツを記録した記録装置を特定することができる。

また、同様に再生装置が再生時に、自身の装置IDを電子透かしとして、記録媒体上のコンテンツに埋め込む構成であってもよい。このとき、装置IDが埋め込まれたコンテンツが不正流出した場合に、コンテンツから、埋め込まれた装置IDを抽出することにより、そのコンテンツを再生した再生装置を特定することができる。

(11) コンテンツ供給システムは、暴露されたデバイス鍵を持つ不正装置が発見された場合に、内部に格納されているデバイス鍵を特定することができるデバイス鍵発見装置を含むとしてもよい。この不正装置は、再生装置200と同じ構成を有している。

デバイス鍵発見装置は、図8に示すように、 n 枚の記録媒体MD1、MD2、MD3、・・・、MD n を生成する。なお、図8では、メディア鍵データ以外の他のデータについては、図示を省略している。

記録媒体MD1、MD2、MD3、・・・、MD n は、以下の点を除いて、第3に示す記録媒体120と同じ内容のデータを記録している。

(a) 記録媒体MD 1、MD 2、MD 3、・・・、MD nに記録されている無効化リストCRLに登録されている無効化された公開鍵証明書はない。つまり、無効化リストCRLは、公開鍵証明書の識別子を含んでいない。

(b) 記録媒体MD 1、MD 2、MD 3、・・・、MD nに記録されている
5 各メディア鍵データは、記録媒体120に記録されているメディア鍵データとは異なるものである。記録媒体MD 1、MD 2、MD 3、・・・、MD nに記録されている各メディア鍵データの一例を図8に示す。

(b-1) 記録媒体MD 1に記録されているメディア鍵データは、n個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号
10 については、第1の実施の形態において説明した通りである。

第1の暗号化メディア鍵は、デバイス鍵DK__1を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

第2、第3、・・・、第nの暗号化メディア鍵は、それぞれ、デバイス鍵DK__2、DK__3、・・・、DK__nを用いて、値「0」に暗号化アルゴリズム
15 ムE1を施して生成されたものである。

(b-2) 記録媒体MD 2に記録されているメディア鍵データは、n個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号については、第1の実施の形態において説明した通りである。

第1の暗号化メディア鍵は、デバイス鍵DK__1を用いて、値「0」に暗号
20 化アルゴリズムE1を施して生成されたものである。

第2の暗号化メディア鍵は、デバイス鍵DK__2を用いて、メディア鍵MKに暗号化アルゴリズムE1を施して生成されたものである。

第3、・・・、第nの暗号化メディア鍵は、それぞれ、デバイス鍵DK__3、・・・、DK__nを用いて、値「0」に暗号化アルゴリズムE1を施して生成されたも
25 のである。

(b-3) 記録媒体MD 3、・・・、MD nについて、上記と同様である。

整数i ($1 \leq i \leq n$) について、記録媒体MD iに記録されているメディア鍵データは、n個の組から構成される。各組は、暗号化メディア鍵と装置番号とを含む。装置番号については、第1の実施の形態において説明した通りであ
30 る。

第 i の暗号化メディア鍵は、デバイス鍵 DK_i を用いて、値「0」に暗号化アルゴリズム $E1$ を施して生成されたものである。

その他の暗号化メディア鍵は、対応するデバイス鍵を用いて、メディア鍵 MK に暗号化アルゴリズム $E1$ を施して生成されたものである。

- 5 次に、操作者は、記録媒体 $MD1$ 、 $MD2$ 、 $MD3$ 、 \dots 、 MDn を一枚ずつ順に、不正装置に装着し、コンテンツの再生を不正装置に対して指示する。

こうして、 n 枚の記録媒体が不正装置により試される。

不正装置によりコンテンツが正しく再生された場合に、装着された記録媒体により、不正装置が内蔵するであろうデバイス鍵を特定することができる。

- 10 例えば、記録媒体 $MD1$ が装着された場合に、不正装置によりコンテンツが正しく再生されたのであれば、不正装置が内蔵するデバイス鍵は、 DK_1 である。

一般化して言うと、記録媒体 MDi が装着された場合に、不正装置によりコンテンツが正しく再生されたのであれば、不正装置が内蔵するデバイス鍵は、

- 15 DK_i である。

不正装置は、再生装置 200 と同じ構成を有しており、図6～図7に示すように動作するので、記録媒体 $MD1$ 、 $MD2$ 、 $MD3$ 、 \dots 、 MDn のいずれか一枚が装着された場合に限り、コンテンツを正しく再生する。

- (12) 第1の実施の形態では、署名生成アルゴリズムとして、署名対象データにその署名を付与する付録型署名を用いるとしているが、本発明は、この構成に限定されるものではない。
- 20

例えば、メッセージ付録型署名ではなく、メッセージ回復型署名を使用するとしてもよい。なお、メッセージ回復型署名については、特許文献3に開示されている。

- 25 メッセージ回復型署名では、署名者が、生成する署名に秘密情報を埋め込むことが可能であり、検証者が、署名検証後にその秘密情報を得ることが可能である。この特徴を利用して、記録装置は、秘密情報と鍵データ（例えばコンテンツ鍵）とに XOR 演算（排他的論理和）を施し、演算結果に対して、メッセージ回復型署名を施して署名データを生成する。このとき、再生装置は、署名
- 30 検証をし、検証が成功した場合に、前記演算結果を得、内蔵している秘密情報

と演算結果に対して、XOR演算（排他的論理和）を施して、鍵データ（例えばコンテンツ鍵）を得る。

- 5 なお、秘密情報と鍵データとの間の演算は、XOR演算に限定する必要はなく、加算演算や、両データを結合したデータを入力値として、ハッシュ関数の出力値を利用する構成であってもよい。

また、秘密情報を作用させる情報は、コンテンツ鍵である必要はなく、鍵暗号化鍵などの他の鍵であってもよい。

- 10 以上のように、署名検証することで得られる秘密情報を獲得しない限り、コンテンツの再生が行えない構成であれば如何なる構成であってもよい。このように、メッセージ回復型署名を利用することで、コンテンツの再生には署名検証が必須となる。

（１３）第１の実施の形態では、コンテンツ鍵及びコンテンツは、記録装置の外部から取得するとしているが、本発明は、この構成に限定されるものではない。

- 15 例えば、コンテンツ記録装置内部に、予めコンテンツ鍵及びコンテンツを対応付けて格納しているとしてもよい。また、コンテンツ鍵を、利用の都度、記録装置内部で生成するとしてもよい。

- （１４）第１の実施の形態では、種々の検証、並びに判定結果に基づいて制御されるスイッチ２１３は、復号部２０５と再生部２１４との間に備えられ、
20 再生部２１４に対して復号コンテンツの出力を行うか否かを制御するとしているが、本発明は、この構成に限定されるものではない。

例えば、スイッチ２１３は、復号部２０４と復号部２０５との間に備えられ、復号部２０５に対して復号コンテンツ鍵の出力を行うか否かを制御するとしてもよい。

- 25 また、スイッチ２１３は、鍵計算部２０３と復号部２０４との間に備えられ、復号部２０４に対して、鍵復号鍵KDKの出力を行うか否かを制御するとしてもよい。

- 30 このように、各検証の結果に基づき、最終的なコンテンツの再生を制御できる構成であれば如何なる構成であってもよい。さらに、スイッチ２１３は物理的なスイッチである必要はなく、再生制御を行える構成であれば、ソフトウェア

アによる構成であってもよい。

- また、鍵計算部202は、生成した復号メディア鍵yが、検知情報である値「0」であるか否かを判断し、復号メディア鍵yが値「0」であると判断する場合に、スイッチ213に対して、復号コンテンツDCNTを再生部214へ
- 5 出力しないように指示するとしてもよい。

また、鍵計算部202は、復号メディア鍵yが値「0」であると判断する場合に、鍵計算部203、復号部204、復号部205の全て又はいずれかに対して、鍵復号鍵の生成、復号コンテンツ鍵の生成、復号コンテンツの生成を行わないように指示するとしてもよい。

- 10 また、鍵計算部202は、復号メディア鍵yが値「0」であると判断する場合に、制御部215に対して、復号メディア鍵yが値「0」である旨のメッセージを通知し、制御部215は、前記メッセージを受け取ると、再生装置200を構成する他の構成要素に対して、暗号化コンテンツの復号及び再生を中止するように指示するとしてもよい。

- 15 (15) 第1の実施の形態では、メディア鍵、鍵暗号化鍵及びコンテンツ鍵の3階層から暗号化システムを採用しているが、本発明は、この構成に限定されるものではない。

- 例えば、コンテンツ鍵を省き、鍵暗号化鍵で直接コンテンツを暗号化する構成であってもよい。あるいは、新たな鍵を導入してその階層を1階層増やす構
- 20 成であってもよい。

(16) 記録装置又は再生装置は、インターネットに代表されるネットワークを介して、メディア鍵データ及び無効化リストCRLの最新版を取得し、内蔵するデータを更新する構成であってもよい。

- 25 (17) 第1の実施の形態では、記録装置が無効化リストCRLを記録媒体に記録するとしているが、本発明は、この構成に限定されるものではない。

例えば、再生装置は、無効化リストCRLを、ネットワークを介して取得するものとして、記録装置は、CRLを記録媒体に記録しない構成であってもよい。

- 30 (18) 第1の実施の形態では、記録装置が、記録媒体に記録するコンテンツ又はコンテンツに関連する情報に対して署名データを生成し、生成した署名

データを記録媒体に記録するとしているが、本発明は、この構成に限定されるものではない。

例えば、記録装置は、署名生成を行わないとしてもよい。このとき、記録装置は、自身が保有するメディア鍵データ及び媒体固有番号に基づいてコンテンツを暗号化して、暗号化に使用したメディア鍵データと、暗号化されたコンテンツを記録媒体に記録するとしてもよい。このとき、再生装置は、記録媒体からメディア鍵データ、媒体固有番号、及び暗号化コンテンツを読み出し、メディア鍵データ、及び媒体固有番号に基づいてコンテンツを復号する。

(19) 第1の実施の形態では、記録装置は、メディア鍵及び媒体固有番号から鍵暗号化鍵を生成することにより、メディアバインドを実現しているが、本発明は、この構成に限定されるものではない。

例えば、記録装置は、メディア鍵及び媒体固有番号に基づいて認証子を生成して、生成した認証子を記録媒体に記録することにより、メディアバインドを実現するとしてもよい。このとき、再生装置は、同じく、メディア鍵及び媒体固有番号から認証子を生成し、記録媒体に記録された認証子と、生成した認証子が一致するか否かを判定してコンテンツの再生を制御する。

上記の認証子の生成方法は、一例として、次の通りである。

メディア鍵、媒体固有番号及び暗号化コンテンツ鍵を結合した値に、ハッシュ関数を施し、得られたハッシュ値、又はハッシュ値の特定の一部を認証子とする。

(20) 第1の実施の形態では、1枚の記録媒体は、1個のコンテンツ供給システムのみに対応しているが、本発明は、この構成に限定されるものではない。

複数のコンテンツ供給システムが存在し、例えば、1のコンテンツ供給システムは、映画のコンテンツを供給するシステムである。別のコンテンツ供給システムは、コンピュータソフトウェアを供給するシステムである。さらに別のコンテンツ供給システムは、音楽を供給するシステムである。このように、供給されるコンテンツの種類により、異なるコンテンツ供給システムが用いられる。

また、例えば、1のコンテンツ供給システムは、映画供給業者Aにより、映

画のコンテンツを供給するシステムである。別のコンテンツ供給システムは、映画供給業者Bにより、映画のコンテンツを供給するシステムである。さらに別のコンテンツ供給システムは、映画供給業者Cにより、映画のコンテンツを供給するシステムである。このように、コンテンツの供給者により、異なるコンテンツ供給システムが用いられることもある。

ここでは、1枚の記録媒体が、異なる複数のコンテンツ供給システムにおいて利用される仕組みについて、説明する。

記録媒体の書き換え不可領域には、記録媒体に固有の媒体固有番号に加え、鍵の無効化データが予め記録されている。このとき、第1のコンテンツ供給システムは、予め書き換え不可領域に記録されている鍵の無効化データを使用することにより、著作物保護の仕組みを実現する。また、第2のコンテンツ供給システムは、第1の実施の形態に示した構成で、著作物保護の仕組みを実現する。

図9に、前記記録媒体に記録されるデータの一例を示す。

記録媒体700には、書き換え不可領域710と、書き換え可能領域720が存在し、書き換え不可領域710には、第1のコンテンツ供給システム用の鍵無効化データ記録領域711と、固有番号記録領域712が存在する。また、書き換え可能領域720には、第2のコンテンツ供給システム用の鍵無効化データ記録領域721と、第1の暗号化コンテンツ鍵記録領域722と、第2の暗号化コンテンツ鍵記録領域723と、その他の暗号化コンテンツ記録領域(図示していない)とが存在する。

ここで、第2のコンテンツ供給システム用の鍵無効化データ記録領域721は、第1の実施の形態におけるメディア鍵データ記録領域122に相当する。さらに、第1の暗号化コンテンツ鍵記録領域722には、第1のコンテンツ供給システム用の鍵無効化データに基づいて暗号化されたデータが記録され、同様に、第2の暗号化コンテンツ鍵記録領域723には、第2のコンテンツ供給システム用の鍵無効化データに基づいて暗号化されたデータが記録される。

このように、1つの記録媒体が複数のコンテンツ供給システムをサポートする場合、媒体固有番号はシステムごとに複数存在する必要はなく、記録媒体に唯一でよく、各コンテンツ供給システムが同一の媒体固有番号、あるいはその

一部分を共通に使用する構成であってもよい。

ここで、媒体固有番号の一部を使用するとは、例えば128ビットの媒体固有番号が存在した場合に、上位32ビットは使用せず、下位96ビットを媒体固有番号として使用したり、媒体固有番号の上位32ビットをオール0に置き換え、128ビットの媒体固有番号として使用したりすることを意味する。

以上のように、記録媒体に予め記録されている媒体固有番号を複数のコンテンツ供給システムで共通に使用することにより、既に市販され利用されている媒体固有番号のみを記録した記録媒体においても、著作物の著作権を保護することができるシステムの実現が可能となる。また、システムごとに媒体固有番号を記録する必要がないことにより、書き換え不可領域の容量削減も可能である。

以上のように、本発明は、少なくとも第1及び第2のコンテンツ供給システムに対して著作物保護の仕組みを提供する著作物保護システムである。

記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号と、第1のコンテンツ供給システム用に鍵無効化データとが予め記録されている。

第1のコンテンツ供給システムは、前記記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成されている。前記複数の再生装置のうちいずれか1台以上は、無効化されている。前記記録媒体の前記書換不可領域に記録されている前記鍵無効化データは、前記無効化された再生装置の鍵を示している。

前記記録装置は、前記書換不可領域に記録されている前記無効化データを用いて、コンテンツを暗号化する暗号化部と、生成した暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込部とを備える。

前記再生装置は、前記記録媒体の前記書換不可領域に記録されている前記鍵無効化データと、前記記録媒体に記録されている前記暗号化コンテンツを読み出す読出部と、読み出した前記鍵無効化データを用いて、前記暗号化コンテンツの復号を許可するか否かを判断する判断部と、復号が許可されない場合に、

前記暗号化コンテンツの復号を禁止し、復号が許可される場合に、前記暗号化コンテンツを復号して、復号コンテンツを生成する復号部とを備える。

また、第2のコンテンツ供給システムは、前記記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成されている。前記複数の再生装置のうちいずれか1台以上は、無効化されている。

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶部と、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出部と、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成部と、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化部と、前記記憶部から前記メディア鍵データを読み出す読出部と、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込部とを備える。

各再生装置は、前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出部と、当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号部と、生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御部と、復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号部とを備える。

1. 8 まとめ

以上説明したように、本発明は、コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体から暗号化コ

ンテンツを読み出して復号する再生装置からなる著作権保護システムである。

前記記録装置は、特定装置が保有する鍵を無効化するための無効化データを保持して、前記無効化データに基づいて前記コンテンツを暗号化して、前記記録媒体に、前記無効化データ、並びに前記暗号化コンテンツを記録して、さらに、前記コンテンツ、あるいは前記コンテンツの暗号化に関連するデータに対して署名を生成して、前記生成した署名を前記記録媒体に記録する。

前記記録媒体は、ユーザにより書き換えできない領域に、前記記録媒体を一意に識別する識別番号を記録して、さらに、前記無効化データ、前記暗号化コンテンツ、並びに前記署名を記録する。

10 前記再生装置は、前記記録媒体から、前記無効化データ、前記暗号化コンテンツ、並びに前記署名を読み出して、前記無効化データに基づいて前記コンテンツを復号して、前記署名の正当性を検証した結果に基づいて、前記復号したコンテンツの再生を制御するとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録媒体は、前記無効化データ、並びに前記暗号化コンテンツを記録して、前記署名は、前記記録媒体とは異なる記録媒体、あるいは通信媒体を介して配布されるとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録装置は、2つ以上の装置の組み合わせで処理を行い、前記装置ごとに処理を分担するとしてもよい。

ここで、前記著作権保護システムにおいて、前記再生装置は、2つ以上の装置の組み合わせで処理を行い、前記装置ごとに処理を分担するとしてもよい。

ここで、前記著作権保護システムにおいて、前記記録装置は、コンテンツの利用条件に基づいてコンテンツを記録するとしてもよい。

ここで、前記著作権保護システムにおいて、前記再生装置は、コンテンツの利用条件に基づいてコンテンツを再生するとしてもよい。

25 ここで、前記著作権保護システムにおいて、前記記録装置は、前記記録装置を一意に識別する装置特定番号を保持して、コンテンツの記録に際して、前記装置特定番号を電子透かしとして前記コンテンツに埋め込むとしてもよい。

ここで、前記著作権保護システムにおいて、前記再生装置は、前記再生装置を一意に識別する装置特定番号を保持して、コンテンツの再生に際して、前記装置特定番号を電子透かしとして前記コンテンツに埋め込むとしてもよい。

ここで、前記著作権保護システムにおいて、不正装置が発見された際に、前記不正装置が保有する鍵の種類を判定する鍵発見装置を含むとしてもよい。

- また、本発明は、コンテンツを暗号化して記録する記録装置である。前記記録装置は、特定装置が保有する鍵を無効化するための無効化データを保持して、
- 5 前記無効化データに基づいて前記コンテンツを暗号化して、記録媒体に、前記無効化データ、並びに前記暗号化コンテンツを記録して、さらに、前記コンテンツ、あるいは前記コンテンツの暗号化に関連するデータに対して署名を生成して、前記生成した署名を前記記録媒体に記録する。

- ここで、前記記録装置は、前記無効化データに加えて、前記記録媒体を一意
- 10 に識別する識別番号に基づいて前記コンテンツを暗号化するとしてもよい。

ここで、前記記録装置は、前記署名の生成に使用した秘密鍵に対応する公開鍵を前記記録媒体に記録するとしてもよい。

ここで、前記記録装置は、公開鍵の無効化リストを署名対象として署名生成を行うとしてもよい。

- 15 ここで、前記記録装置は、前記コンテンツを記録する記録媒体に無効化データが存在する場合に、前記記録装置が保有する無効化データと、前記記録媒体に存在する無効化データの新旧を比較して、新しい無効化データを保有するとしてもよい。

- ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化データの
- 20 のサイズの比較で行い、サイズの大きい無効化データを新しいと判断するとしてもよい。

ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化している鍵数の比較で行い、無効化している鍵数が多い無効化データを新しいと判断するとしてもよい。

- 25 ここで、前記記録装置は、前記無効化データの新旧の比較を、無効化データの生成日、あるいはバージョン番号の比較で行い、前記生成日、あるいは前記バージョン番号は、改ざんから保護されているとしてもよい。

- ここで、前記記録装置は、前記コンテンツを記録する記録媒体に無効化データ、並びに暗号化コンテンツが存在して、かつ、前記記録装置が保有する無効
- 30 化データが、前記記録媒体に記録されている無効化データと比較して新しい場

合に、前記記録媒体に記録された前記暗号化コンテンツを、同様に、前記記録媒体に記録された無効化データに基づいて一旦復号して、前記記録装置が保有する無効化データに基づいて再暗号化するとしてもよい。

5 ここで、前記記録装置は、前記記録装置内部で秘密情報を生成して、前記秘密情報と前記無効化データに基づいて前記コンテンツを暗号化して、前記秘密情報を署名に埋め込む情報として署名を生成するとしてもよい。

10 また、本発明は、記録媒体から暗号化コンテンツを読み出して復号する再生装置である。前記再生装置は、前記記録媒体から、無効化データ、前記暗号化コンテンツ、並びに署名を読み出して、前記無効化データに基づいて前記コンテンツを復号して、前記署名の正当性を検証した結果に基づいて、前記復号したコンテンツの再生を制御する。

ここで、前記再生装置は、前記無効化データに加えて、前記記録媒体を一意に識別する識別番号に基づいて前記暗号化コンテンツを復号するとしてもよい。

15 ここで、前記再生装置は、公開鍵の無効化リストを保有して、前記無効化リストを使用して、前記署名の正当性の検証に使用する公開鍵が、前記無効化リストに登録されているか否かを判断して、前記判断した結果に基づいて、前記復号したコンテンツの再生を制御するとしてもよい。

20 ここで、前記再生装置は、前記記録媒体に前記無効化リストが存在する場合には、前記再生装置が保有する無効化リストと、前記記録媒体に存在する無効化リストの新旧を比較して、新しい無効化リストを保有するとしてもよい。

ここで、前記再生装置は、前記無効化リストの新旧の比較を、無効化リストのサイズの比較で行い、サイズの大きい無効化リストを新しいと判断するとしてもよい。

25 ここで、前記再生装置は、前記無効化リストの新旧の比較を、無効化している公開鍵数の比較で行い、無効化している公開鍵数が多い無効化リストを新しいと判断するとしてもよい。

ここで、前記再生装置は、前記署名の正当性の検証を行うことにより秘密情報を獲得して、前記獲得した秘密情報、並びに無効化データに基づいて、前記暗号化コンテンツを復号するとしてもよい。

30 また、本発明は、暗号化コンテンツを記録する記録媒体である。前記記録媒

体は、ユーザにより書き換えできない領域に、前記記録媒体を一意に識別する識別番号を記録して、さらに、無効化データ、暗号化コンテンツ、並びに署名を記録している。

ここで、前記記録媒体は、前記無効化データ、並びに識別番号に基づいて暗号化されたコンテンツを記録しているとしてもよい。

ここで、前記記録媒体は、前記署名の生成に使用した秘密鍵に対応する公開鍵を記録しているとしてもよい。

ここで、前記記録媒体は、2つ以上の記録装置により記録された場合に、2つ以上の無効化データ、並びに2つ以上の公開鍵を記録しているとしてもよい。

10 以上、説明したように、第1の実施の形態においては、記録装置が、メディア鍵データから算出されるメディア鍵に基づいてコンテンツを暗号化し、かつ記録装置自身の公開鍵証明書及び生成した署名を合わせて記録媒体に記録することで、記録媒体の書き換え不可領域に鍵無効化情報が記録されていない記録媒体であっても、鍵無効化及びメディアバインドを実現して、不正装置を使っ
15 たコンテンツの記録又は再生による著作物侵害の防止を実現することができ
る。

具体的には、正規の記録装置及び不正な再生装置が存在する場合、正規の記録装置は、不正な再生装置の無効化を示すメディア鍵データに基づいてコンテンツを暗号化して記録媒体に記録する。その記録媒体を挿入した不正な再生装置は、記録されているメディア鍵データからはメディア鍵を復号することができ
20 ないため、不正な再生装置によるコンテンツの再生を防止できる。

また、不正な記録装置及び正規の再生装置が存在する場合、不正な記録装置は、自身が無効化されていない古いメディア鍵データに基づいてコンテンツを暗号化して記録媒体に記録する。このとき、記録装置自身の公開鍵証明書及び生成した署名データも記録する。その記録媒体を挿入した正規の再生装置は、記録されているメディア鍵データからメディア鍵を復号することができる。しかし、コンテンツの再生前に記録装置の公開鍵証明書が無効化リストCRLに登録されているか否かを判断するため、無効化リストCRLに登録されている不正な記録装置により記録されたコンテンツであれば、その再生を止めること
25 ができる。
30

2. 第2の実施の形態

本発明に係る別の実施の形態としてのコンテンツ供給システム20について説明する。

2. 1 コンテンツ供給システム20の構成

5 コンテンツ供給システム20は、コンテンツ供給システム10と類似した構成を有しており、図10に示すように、配信局装置1400、コンテンツサーバ装置1500、記録装置1100及び再生装置1200a、1200b、1200c、1200d、1200e、・・・から構成されている。

第1の実施の形態と同様に、再生装置のうちの一部は、無効化されている。

10 2. 2 配信局装置1400

配信局装置1400は、情報記憶部1401、制御部1402、入力部1403、表示部1404及び送受信部1405から構成されている（図示していない）。

15 配信局装置1400は、具体的には、第1の実施の形態のコンテンツサーバ装置500と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、通信ユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、配信
20 局装置1400の各構成要素は、その機能を達成する。

送受信部1405は、インターネット40を介して、記録装置1100と接続されており、記録装置1100と制御部1402との間で情報の送受信を行う。

25 情報記憶部1401は、鍵無効化データRDATAとバージョン番号VRとを対応付けて予め記憶している。

鍵無効化データRDATAは、第1の実施の形態のメディア鍵データMDATAと同一である。ここでは、詳細の説明を省略する。

バージョン番号VRは、当該バージョン番号VRに対応する鍵無効化データRDATAの世代を示す情報である。

30 制御部1402は、記録装置1100から、インターネット40及び送受信

部1405を介して、鍵無効化データRDATAの取得要求を受け取る。前記取得要求を受け取ると、制御部1402は、情報記憶部1401から、鍵無効化データRDATAとバージョン番号VRとを読み出し、読み出した鍵無効化データRDATAとバージョン番号VRとを、送受信部1405及びインターネット40を介して、記録装置1100へ送信する。

入力部1403は、配信局装置1400の操作者の指示を受け付け、受け付けた指示を制御部1402へ出力する。

表示部1404は、制御部1402の制御により、様々な情報を表示する。

2. 3 コンテンツサーバ装置1500

10 コンテンツサーバ装置1500は、第1の実施の形態のコンテンツサーバ装置500と同一の構成を有している。ここでは、説明を省略する。

2. 4 記録装置1100

記録装置1100は、図11に示すように、デバイス鍵格納部1101、無効化データ格納部1102、鍵計算部1103、暗号化部1105、暗号化部1106、認証子生成部1104、割当部1107、比較部1108、制御部1109、ドライブ部1110及び送受信部1111から構成されている。

記録装置1100は、具体的には、記録装置100と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、記録装置1100は、その機能を達成する。

(1) デバイス鍵格納部1101

25 デバイス鍵格納部1101は、外部の装置からアクセスできないように、デバイス鍵DK__1を秘密に記憶している。デバイス鍵DK__1は、記録装置1100に固有の鍵である。

(2) 無効化データ格納部1102

無効化データ格納部1102は、配信局装置1400から取得した鍵無効化データRDATAとバージョン番号VRとを記憶するための領域を有している。

30 (3) 鍵計算部1103

鍵計算部1103は、第1の実施の形態の鍵計算部103と同様の構成を有している。

5 鍵計算部1103は、無効化データ格納部1102から鍵無効化データRD
ATAを読み出し、デバイス鍵格納部1101からデバイス鍵DK₁を読み
出す。次に、鍵計算部103と同様に、読み出したデバイス鍵DK₁を用い
て、読み出した鍵無効化データRDATAに復号アルゴリズムD1を施してメ
ディア鍵MKを生成し、生成したメディア鍵MKを認証子生成部1104及び
暗号化部1105へ出力する。

(4) 暗号化部1105

10 暗号化部1105は、コンテンツサーバ装置1500から、送受信部111
1を介して、コンテンツ鍵CKを受け取り、鍵計算部1103からメディア鍵
MKを受け取る。

次に、暗号化部1105は、受け取ったメディア鍵MKを用いて、受け取っ
たコンテンツ鍵CKに暗号化アルゴリズムE2を施して、暗号化コンテンツ鍵
15 ECKを生成する。

暗号化コンテンツ鍵ECK=E2 (MK, CK)

次に、暗号化部1105は、ドライブ部1110を介して、記録媒体130
0上の暗号化コンテンツファイル1320内に鍵記録部1323を確保し、次
に、生成した暗号化コンテンツ鍵ECKを、ドライブ部1110を介して、鍵
20 記録部1323へ書き込む。

また、暗号化部1105は、生成した暗号化コンテンツ鍵ECKを認証子生
成部1104へ出力する。

(5) 暗号化部1106

25 暗号化部1106は、コンテンツサーバ装置1500から、送受信部111
1を介して、コンテンツ鍵CK及びコンテンツCNTを受け取り、受け取った
コンテンツ鍵CKを用いて、受け取ったコンテンツCNTに暗号化アルゴリズム
E3を施して暗号化コンテンツECNTを生成する。

暗号化コンテンツECNT=E3 (CK, CNT)

次に、暗号化部1106は、ドライブ部1110を介して、記録媒体130
30 0上の暗号化コンテンツファイル1320内にコンテンツ記録部1324を確

保し、次に、生成した暗号化コンテンツECNTを、ドライブ部1110を介して、コンテンツ記録領域124へ書き込む。

(6) 認証子生成部1104

5 認証子生成部1104は、鍵計算部1103からメディア鍵MKを受け取り、暗号化部1105から暗号化コンテンツ鍵ECKを受け取り、記録媒体1300の固有番号記録領域1301から媒体固有番号MIDを読み出す。

次に、認証子生成部1104は、受け取ったメディア鍵MKと、読み出した媒体固有番号MIDと、受け取った暗号化コンテンツ鍵ECKとをこの順序で結合して、結合データを生成し、生成した結合データに一方方向性関数Fを施して、認証子MAC (Message Authentication Code) を生成する。

$$MAC = F (MK || ECK || MID)$$

ここで、F(A)は、データAに対して一方方向性関数Fを施して得られた値を示している。また、一方方向性関数Fの一例は、ハッシュ関数SHA-1である。

15 次に、認証子生成部1104は、ドライブ部1110を介して、記録媒体1300上の暗号化コンテンツファイル1320内に認証子記録部1322を確保し、生成した認証子MACを、ドライブ部1110を介して、認証子記録部1322に書き込む。

20 このようにして生成された認証子MACは、再生装置1200においてコンテンツの正当性を判定する際に用いられる。

(7) 割当部1107

割当部1107は、記録媒体1300に記録する鍵無効化データRDATAに対して、記録媒体1300においてその鍵無効化データRDATAを一意に識別する鍵無効化データ識別子RIDを生成する。次に、ドライブ部1110を介して、記録媒体1300上の暗号化コンテンツファイル1320内に識別子記録部1321を確保し、生成した鍵無効化データ識別子RIDを、ドライブ部1110を介して、識別子記録部1321に書き込む。

なお、割当部1107による鍵無効化データ識別子RIDの具体的な割当方法については後述する。

30 (8) 比較部1108

比較部 1108 は、制御部 1109 の指示により、ドライブ部 1110 を介して、記録媒体 1300 に鍵無効化データファイルが存在するか否かを確認する。次に、ドライブ部 1110 から鍵無効化データファイルが存在するか否かを示す存否情報を受け取る。

- 5 受け取った存否情報が、記録媒体 1300 に鍵無効化データファイルが存在しないことを示す場合には、比較部 1108 は、割当部 1107 に対して、鍵無効化データ識別子 R I D の生成を指示し、また、ドライブ部 1110 に対して、無効化データ格納部 1102 に記録されている鍵無効化データ R D A T A と、そのバージョン番号 V R と、割当部 1107 により生成された鍵無効化データ識別子 R I D とから構成される鍵無効化データファイルを記録媒体 1300 に書き込むように指示する。

- 15 前記存否情報が、記録媒体 1300 に鍵無効化データファイルが存在することを示す場合には、比較部 1108 は、ドライブ部 1110 を介して、記録媒体 1300 上の各鍵無効化データファイルから鍵無効化データ F D A T A に含まれているバージョン番号 V F を読み出す。この場合に、1 個以上のバージョン番号 V F が読み出される。また、無効化データ格納部 1102 から鍵無効化データ R D A T A に対応するバージョン番号 V R を読み出す。

- 20 次に、比較部 1108 は、読み出したバージョン番号 V R と同じ内容のバージョン番号が、読み出した 1 個以上のバージョン番号 V F の中に存在するか否かを判断し、存在しないと判断する場合に、上記と同様に、割当部 1107 に対して、鍵無効化データ識別子 R I D の生成を指示し、また、ドライブ部 1110 に対して、無効化データ格納部 1102 に記録されている鍵無効化データ R D A T A と、そのバージョン番号 V R と、割当部 1107 により生成された鍵無効化データ識別子 R I D とから構成される鍵無効化データファイルを記録媒体 1300 に書き込むように指示する。

存在すると判断する場合に、比較部 1108 は、読み出したバージョン番号 V R と同じ内容のバージョン番号が存在することを示す情報を制御部 1109 へ出力する。

(9) 制御部 1109

- 30 制御部 1109 は、送受信部 1111 及びインターネット 40 を介して、配

信局装置 1400 に対して、鍵無効化データ RDATA の取得要求を送信する。
また、制御部 1109 は、送受信部 1111 を介して、コンテンツサーバ装置
1500 に対して、コンテンツの取得要求を送信する。

制御部 1109 は、比較部 1108 に対して、記録媒体 1300 に鍵無効化
5 データファイルが存在するか否かを確認するように指示する。

比較部 1108 からバージョン番号 VR と同じ内容のバージョン番号が存在
することを示す情報を受け取った場合には、ドライブ部 1110 に対して、記
録媒体 1300 上において、バージョン番号 VR と同じ内容のバージョン番号
を含む鍵無効化データファイルから鍵無効化データ識別子 RID を読み出すよ
10 うに指示し、ドライブ部 1110 から鍵無効化データ識別子 RID を受け取る。

次に、制御部 1109 は、鍵計算部 1103 に対して、デバイス鍵 DK__1
と鍵無効化データ RDATA とを読み出してメディア鍵 MK を生成するように
指示し、暗号化部 1105 に対して、コンテンツ鍵 CK を暗号化するように指
示し、認証子生成部 1104 に対して、媒体固有番号 MID を読み出して、認
15 証子 MAC を生成するように指示し、暗号化部 1106 に対して、コンテンツ
CNT を暗号化するように指示し、次に、ドライブ部 1110 に対して、記
録媒体 1300 上に暗号化コンテンツファイルを確保するように指示し、認証
子生成部 1104、暗号化部 1105 及び暗号化部 1106 に対して、それぞ
れ、生成された認証子 MAC と、生成された暗号化コンテンツ鍵 ECK と、生
20 成された暗号化コンテンツ ECNT とを記録媒体 1300 上の暗号化コンテン
ツファイル内に書き込むように指示する。また、ドライブ部 1110 に対して、
記録媒体 1300 上の暗号化コンテンツファイル内に、識別子記録部 1303
を確保するように指示し、割当部 1107 により生成された又はドライブ部 1
110 から受け取った鍵無効化データ識別子 RID を識別子記録部 1303 に
25 書き込むように指示する。

(10) 送受信部 1111

送受信部 1111 は、インターネット 40 を介して、配信局装置 1400 と
接続されている。また、専用回線 30 を介して、コンテンツサーバ装置 150
0 と接続されている。

30 送受信部 1111 は、配信局装置 1400 から、インターネット 40 を介し

て、鍵無効化データRDATAとバージョン番号VRとを受信する。鍵無効化データRDATAとバージョン番号VRとを受信すると、受信した鍵無効化データRDATA及びバージョン番号VRを、対応付けて、無効化データ格納部1102へ書き込む。

- 5 また、送受信部1111は、専用回線30を介して、コンテンツサーバ装置1500から、コンテンツ鍵CK及びコンテンツCNTを受信し、受信したコンテンツ鍵CK及びコンテンツCNTを暗号化部1106へ出力し、受信したコンテンツ鍵CKを暗号化部1105へ出力する。

 (11) ドライブ部1110

- 10 ドライブ部1110は、記録装置1100を構成する各構成要素の指示により、記録媒体1300から情報を読み出し、読み出した情報を当該構成要素へ出力する。

 また、ドライブ部1110は、記録装置1100を構成する各構成要素の指示により、記録媒体1300に各領域を確保し、また、各構成要素から情報を
15 受け取り、確保した領域に受け取った前記情報を書き込む。

 (12) キーボード1180及びモニタ1190

 キーボード1180は、記録装置1100の操作者の操作指示を受け付け、受け付けた操作指示に対応する指示情報を制御部1109へ出力する。

 モニタ1190は、制御部1109の制御により様々な情報を表示する。

20 2. 5 記録媒体1300

 記録媒体1300は、記録媒体120と同様に、光ディスクメディアであり、図12に示すように、書換不可領域1308と、書換可能領域1309とから構成されている。

- 書換不可領域1308は、図12に示すように、固有番号記録領域1301
25 を有している。記録媒体1300の製造時に、固有番号記録領域1301には、記録媒体1300に固有の媒体固有番号MIDが記録される。このとき、書換可能領域1309には、何も記録されていない。この図では、媒体固有番号MIDは16進数8桁で表現されており、具体的には、「5」である。

- その後、上述したように、記録装置1100により記録媒体1300上に情
30 報が書き込まれると、書換可能領域1309には、記録装置1100により記

録領域1305と記録領域1306とが確保され、記録領域1305には、1個以上の鍵無効化データファイルが記録され、記録領域1306には、1個以上の暗号化コンテンツファイルが記録される。

一例として、図12に示すように、記録領域1305には、鍵無効化データ
5 ファイル1310が記録され、記録領域1306には、暗号化コンテンツファイル1320が記録される。なお、図12に示す記録媒体1300には、一例として、1個の鍵無効化データファイルと1個の暗号化コンテンツファイルとが記録されているが、1個以上の鍵無効化データファイルと1個以上の暗号化コンテンツファイルとが記録媒体上に記録されることもある。

10 鍵無効化データファイル1310は、図12に示すように、版数記録部1311、識別子記録部1312及びデータ記録部1313から構成されている。

版数記録部1311には、鍵無効化データRDATAの世代を示すバージョン番号が記録されており、識別子記録部1312には、記録装置1100の割
15 当部1107により割り当てられた鍵無効化データ識別子R I Dが記録されており、データ記録部1313には、鍵無効化データRDATAが記録されている。

ここで、バージョン番号、鍵無効化データ識別子R I D及び鍵無効化データRDATAについては、上述した通りである。

図12において、バージョン番号は、16進数4桁で表現されており、具体的には、「3」である。第2の実施の形態では、配信局装置1400から、
20 鍵無効化データのバージョン番号が割当てられる。

図12において、鍵無効化データ識別子は、16進数4桁で表現されており、鍵無効化データ識別子R I Dは、具体的には、「1」である。

また、暗号化コンテンツファイル1320は、図12に示すように、識別子
25 記録部1321、認証子記録部1322、鍵記録部1323及びコンテンツ記録部1324から構成されている。また、暗号化コンテンツファイル1320には、当該ファイルに含まれている暗号化コンテンツを識別するコンテンツ番号が付加されている（図示していない）。

識別子記録部1321には、鍵無効化データ識別子R I Dが記録されている。
30 鍵無効化データ識別子R I Dは、コンテンツの暗号化において使用された鍵無

効化データに対して、記録装置1100の割当部1107により割り当てられたものである。

認証子記録部1322には、認証子MACが記録されている。認証子MACは、記録装置1100の認証子生成部1104により生成されたものである。

- 5 鍵記録部1323には、記録装置1100の暗号化部1105により、生成された暗号化コンテンツ鍵ECKが記録されている。

コンテンツ記録部1324には、記録装置1100の暗号化部1106により、生成された暗号化コンテンツECNTが記録されている。

2. 6 再生装置1200

- 10 再生装置1200a、1200b、1200c、・・・は、同様の構成を有しているので、ここでは、再生装置1200として説明する。

再生装置1200は、図13に示すように、デバイス鍵格納部1201、鍵計算部1202、認証子生成部1203、復号部1204、復号部1205、比較部1206、指定受付部1207、取得部1208、検索部1209、ス
15 イッチ1211、ドライブ部1213、再生部1214、制御部1215、入力部1216及び表示部1217から構成されている。

再生装置1200は、具体的には、再生装置200と同様に、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コ
20 ンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、再生装置1200は、その機能を達成する。

(1) 指定受付部1207

指定受付部1207は、利用者から、リモコン1280及び入力部1216
25 を介して、再生すべきコンテンツの指定を受け付け、指定を受け付けたコンテンツを識別するコンテンツ番号を取得部1208及び認証子生成部1203へ出力する。

(2) 取得部1208

取得部1208は、指定受付部1207からコンテンツ番号を受け取り、ド
30 ライブ部1213を介して、記録媒体1300の記録領域1305より、受け

取ったコンテンツ番号が付加された暗号化コンテンツファイル1320を見出し、見出した暗号化コンテンツファイル1320の識別子記録部1321から、鍵無効化データ識別子R I Dを読み出す。次に、読み出した鍵無効化データ識別子R I Dを検索部1209へ出力する。

5 (3) 検索部1209

検索部1209は、取得部1208から鍵無効化データ識別子R I Dを受け取る。鍵無効化データ識別子R I Dを受け取ると、ドライブ部1213を介して、記録媒体1300の記録領域1305に記録された1個以上の鍵無効化データファイルから、受け取った鍵無効化データ識別子R I Dと同じ内容の鍵無効化データ識別子を識別子記録部に含む鍵無効化データファイルを検索し、検索された鍵無効化データファイルのデータ記録部より、鍵無効化データR D A T Aを読み出す。

次に、検索部1209は、読み出した鍵無効化データR D A T Aを鍵計算部1202へ出力する。

15 (4) デバイス鍵格納部1201

デバイス鍵格納部1201は、デバイス鍵格納部201と同様に、外部の装置からアクセスできないように、デバイス鍵D K _ xを秘密に記憶している。デバイス鍵D K _ xは、再生装置1200に固有の鍵である。

(5) 鍵計算部1202

20 鍵計算部1202は、検索部1209から鍵無効化データR D A T Aを受け取り、デバイス鍵格納部1201からデバイス鍵D K _ xを読み出す。

次に、鍵計算部1202は、鍵計算部202と同様にして、読み出したデバイス鍵D K _ xを用いて、受け取った鍵無効化データR D A T Aに復号アルゴリズムD 1を施して、復号メディア鍵yを生成する。

25 ここで、復号メディア鍵yは、メディア鍵M K 及び値「0」のいずれかである。

次に、鍵計算部1202は、生成した復号メディア鍵yを認証子生成部1203及びスイッチ1211へ出力する。

(6) 認証子生成部1203

30 認証子生成部1203は、鍵計算部1202から復号メディア鍵yを受け取

り、ドライブ部1213を介して、記録媒体1300の固有番号記録領域1301から媒体固有番号MIDを読み出す。また、指定受付部1207からコンテンツ番号を受け取り、ドライブ部1213を介して、記録媒体1300上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル1320を特定し、特定された暗号化コンテンツファイル1320の鍵記録部1323から暗号化コンテンツ鍵ECKを読み出す。

次に、受け取った復号メディア鍵yと、読み出した暗号化コンテンツ鍵ECKと、読み出した媒体固有番号MIDとをこの順序で結合して、結合データを生成し、生成した結合データに一方方向性関数Fを施して、復号認証子DMACを生成する。

$$DMAC = F(y || ECK || MID)$$

次に、認証子生成部1203は、生成した復号認証子DMACを比較部1206へ出力する。

(7) 比較部1206

比較部1206は、認証子生成部1203から復号認証子DMACを受け取る。また、比較部1206は、指定受付部1207からコンテンツ番号を受け取り、ドライブ部1213を介して、記録媒体1300上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル1320を特定し、特定された暗号化コンテンツファイル1320の認証子記録部1322に記録されている認証子MACを読み出す。

次に、比較部1206は、受け取った復号認証子DMACと読み出した認証子MACとが一致するか否かを判断する。一致すると判断する場合に、スイッチ1211へ、閉じる指示を出力し、一致しないと判断する場合に、スイッチ1211へ、開く指示を出力する。

(8) スイッチ1211

スイッチ1211は、比較部1206からの指示により、開閉が制御される。スイッチ1211は、比較部1206から閉じる指示を受け取った場合に、閉じ、開く指示を受け取った場合に、開く。

また、スイッチ1211は、鍵計算部1202から復号メディア鍵yを受け取る。閉じる指示を受け取った場合に、受け取った復号メディア鍵yを復号部

1204へ出力する。開く指示を受け取った場合に、復号メディア鍵yは、外部へ出力されない。

(9) 復号部1204

5 復号部1204は、スイッチ1211から復号メディア鍵yを受け取る。また、指定受付部1207からコンテンツ番号を受け取り、ドライブ部1213を介して、記録媒体1300上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル1320を特定し、特定された暗号化コンテンツファイル1320の鍵記録部1323に記録されている暗号化コンテンツ鍵ECKを読み出し、受け取った復号メディア鍵yを用いて、読み出した暗号化コンテンツ鍵ECKに復号アルゴリズムD2を施して復号コンテンツ鍵DCKを生成し、生成した復号コンテンツ鍵DCKを復号部1205へ出力する。

(10) 復号部1205

15 復号部1205は、復号部1204から復号コンテンツ鍵DCKを受け取る。また、指定受付部1207からコンテンツ番号を受け取り、ドライブ部1213を介して、記録媒体1300上において、受け取った前記コンテンツ番号が付加された暗号化コンテンツファイル1320を特定し、特定された暗号化コンテンツファイル1320のコンテンツ記録部1324に記録されている暗号化コンテンツECNTを読み出し、受け取った復号コンテンツ鍵DCKを用いて、読み出した暗号化コンテンツECNTに復号アルゴリズムD3を施して復号コンテンツDCNTを生成し、生成した復号コンテンツDCNTを再生部1214へ出力する。

(11) 再生部1214

25 再生部1214は、復号部1205から復号コンテンツDCNTを受け取り、受け取った復号コンテンツDCNTから映像情報及び音声情報を生成し、生成した映像情報及び音声情報をアナログの映像信号及び音声信号に変換し、アナログの映像信号及び音声信号をモニタ1290へ出力する。

(12) 制御部1215、入力部1216、表示部1217、ドライブ部1213、モニタ1290及びリモコン1280

30 制御部1215は、再生装置1200を構成する各構成要素の動作を制御する。

リモコン1280は、各種のボタンを備え、操作者の前記ボタンの操作に応じた操作指示情報を生成し、生成した操作指示情報を赤外線に乗せて出力する。

入力部1216は、リモコン1280から、操作指示情報が乗せられた赤外線を受け取り、受け取った赤外線から操作指示情報を抽出し、抽出した操作指

5 示情報を制御部1215又は指定受付部1207へ出力する。

表示部1217は、制御部1215の制御の基に、様々な情報を表示する。

ドライブ部1213は、記録媒体1300からの情報の読み出しを行う。

モニタ1290は、CRT及びスピーカを備え、再生部1214からアナログの映像信号及び音声信号を受信し、映像信号に基づいて映像を表示し、音声

10 信号に基づいて音声を出力する。

2. 7 記録媒体に記録されるデータの構造と関連処理

(1) バージョン番号

図12において、バージョン番号は、16進数4桁で表現されており、具体的には、「3」である。第2の実施の形態では、配信局装置1400から、鍵
15 無効化データのバージョン番号が割当てられる。

具体的には、最初に発行された鍵無効化データには、バージョン番号として「1」が割当てられ、その後、発行される鍵無効化データには、バージョン番号が「2」、「3」、・・・というように割当てられる。

鍵無効化が発生した場合、新しい鍵無効化データが発行され、その際に新しいバージョン番号が付与される。なお、新しい鍵無効化データの発行は、鍵無
20 効化が発生した場合のみに限定されない。例えば、セキュリティの観点から、予め定められた一定期間ごとに新しい鍵無効化データの発行を行うとしてもよい。

(2) 鍵無効化データ識別子

25 図12において、識別子記録部1312に記録されている鍵無効化データ識別子は、16進数4桁で表現されており、鍵無効化データ識別子R I Dは、「1」である。

ここで、鍵無効化データ識別子R I Dは、記録媒体毎に、それぞれ記録される鍵無効化データを一意に識別するための情報である。従って、記録媒体毎に
30 独立した体系により、鍵無効化データ識別子を割り当てることができる。

記録装置 1100 の割当部 1107 による鍵無効化データ識別子 R I D の具体的な割当て方法としては、割当部 1107 は、既に記録媒体に記録されている鍵無効化データに割当てられた鍵無効化データ識別子とは異なる値を割り当てる。

- 5 例えば、図 14 に示すように、記録媒体 1300 a に、既に鍵無効化データファイル 1 と鍵無効化データファイル 2 とが記録されており、それぞれの鍵無効化データ識別子は、「1」及び「2」であるとする。

このとき、この記録媒体に新たな鍵無効化データファイル 3 を記録する際、割当部 1107 は、鍵無効化データ識別子 R I D として、「1」及び「2」以外
10 外の値、例えば「3」を割当てる。

(3) デバイス鍵とメディア鍵

図 12 において、データ記録部 1313 には、 n 個のデバイス鍵 DK_i ($i = 1, 2, \dots, n$) を用いて、メディア鍵 MK を、それぞれ暗号化することにより得られる暗号化メディア鍵 $E(DK_i, MK)$ が記録されている。

- 15 また、図 12 において、装置 n が保有するデバイス鍵を DK_n と表現している。この図の例では、装置 3、並びに装置 4 が無効化されているため、それぞれが保有する DK_3 、及び DK_4 では、メディア鍵 MK とは全く無関係のデータ「0」が暗号化されて記録されている。

鍵無効化データをこのように生成することで、例えば、デバイス鍵 DK_1
20 を保有する装置 1 は、鍵無効化データの $E(DK_1, MK)$ をデバイス鍵 DK_1 で復号することにより、メディア鍵 MK を得ることができるが、デバイス鍵 DK_3 を保有する装置 3 は、鍵無効化データの $E(DK_3, 0)$ をデバイス鍵 DK_3 で復号したとしても、メディア鍵 MK を得ることができない。

このように、図 12 の例では、装置 3 及び装置 4 以外の全ての装置だけが正
25 しいメディア鍵 MK を共有でき、装置 3 及び装置 4 は、正しいメディア鍵 MK が得られない。こうして、無効化された装置 3 及び装置 4 を、システムから排除することができる。

なお、装置の無効化方法は他の方法を利用してもよく、例えば、特許文献 1 には木構造を利用した無効化方法が開示されている。

- 30 (4) 暗号化コンテンツファイル

図12において、暗号化コンテンツファイル1320は、識別子記録部1321、認証子記録部1322、鍵記録部1323及びコンテンツ記録部1324からなる。

この図において、識別子記録部1321に記録されている鍵無効化データ識別子は、16進数4桁で表現されており、鍵無効化データ識別子R I Dは、具体的には、「1」である。

鍵無効化データ識別子R I Dは、以下で説明するように、再生装置1200において、再生したい暗号化コンテンツを復号するために使用する鍵無効化データファイル310を記録媒体1300から取得するために使用される。

10 即ち、再生装置1200において、記録媒体1300に記録された暗号化コンテンツを復号再生する際、再生したい暗号化コンテンツファイル1320の識別子記録部1321に記録されている鍵無効化データ識別子R I Dと同じ鍵無効化I Dを識別子記録部1312に含む鍵無効化データファイル310を、記録媒体1300から取得する。

15 ここで、図15を用いてより具体的に説明する。図15に示すように、記録媒体1300bには、鍵無効化データファイル1、鍵無効化データファイル2、暗号化コンテンツファイルA、暗号化コンテンツファイルB及び暗号化コンテンツファイルCが記録されている。

この図に示すように、鍵無効化データファイル1及び鍵無効化データファイル20の鍵無効化データ識別子は、それぞれ、「1」及び「2」である。また、暗号化コンテンツファイルA、暗号化コンテンツファイルB及び暗号化コンテンツファイルCの鍵無効化データ識別子は、それぞれ、「1」、「1」及び「2」である。

これは、記録装置1100において、暗号化コンテンツファイルAを生成し25記録する際、鍵無効化データファイル1の鍵無効化データを使用し、暗号化コンテンツファイルBを生成し記録する際、鍵無効化データファイル1の鍵無効化データを使用し、暗号化コンテンツファイルCを生成し記録する際、鍵無効化データファイル2の鍵無効化データを使用したことを表している。

このとき、再生装置1200は、例えば、図15に示す記録媒体1300b30における暗号化コンテンツファイルBを復号して再生する場合には、暗号化コ

コンテンツファイルBの鍵無効化データ識別子は「1」であるから、鍵無効化データ識別子が「1」である鍵無効化データファイル1を取得し、所得した鍵無効化データファイル1に含まれている鍵無効化データを使用して、暗号化コンテンツファイルBに格納されている暗号化コンテンツを復号する。

5 2. 8 コンテンツ供給システム20の動作

コンテンツ供給システム20の動作について、特に、記録装置1100による記録媒体1300へのデータの書き込みの動作及び再生装置1200による記録媒体1300に記録されているデータの再生の動作について、説明する。

(1) 記録装置1100による書き込みの動作

10 記録装置1100による記録媒体1300へのデータの書き込みの動作について、図16～図18に示すフローチャートを用いて説明する。

記録装置1100の送受信部1111は、配信局装置1400から、インターネット40を介して、鍵無効化データRDATA及びバージョン番号VRを受信し、受信した鍵無効化データRDATA及びバージョン番号VRを、対応
15 付けて、無効化データ格納部1102に格納する（ステップS1501）。

なお、ステップS1501における鍵無効化データRDATA及びバージョン番号VRの受信は、配信局装置1400により、新しい鍵無効化データRDATAが発行された時に行われる。鍵無効化データRDATAには、上述したように、その発行順序を示すバージョン番号VRが付加されている。記録装置
20 1100は、このバージョン番号VRに基づいて、受信した鍵無効化データRDATAが新しいものかどうかを確認する。

例えば、記録装置1100の無効化データ格納部1102が、バージョン番号「1」が付加された鍵無効化データを保持している場合、配信局装置1400からバージョン番号「2」が付加された鍵無効化データを受信したと想定するとき、記録装置1100の制御部1109は、受信した鍵無効化データに付
25 加されたバージョン番号「2」と、無効化データ格納部1102に保持されている鍵無効化データに付加されたバージョン番号「1」とを比較する。受信した鍵無効化データに付加されたバージョン番号「2」の方が新しいので、制御部1109は、受信した鍵無効化データは、新しいものであるとして、受信し
30 た鍵無効化データとバージョン番号「2」とを無効化データ格納部1102に

格納するように送受信部1111へ指示を行う。ここで、バージョン番号は、その値が大きいほど、新しいことを示しているものとする。

なお、ここでは鍵無効化データの新旧の比較にバージョン番号を用いる場合について説明したが、この方法には限定されない。例えば、バージョン番号の

- 5 代わりに、鍵無効化データには、その発行日時が付加されており、鍵無効化データの発行日時を用いて、鍵無効化データの新旧を比較する構成としてもよい。また、ここでは、配信局装置1400から鍵無効化データを入手するとしたが、鍵無効化データの取得方法はこの構成に限定されない。例えば、鍵無効化データとバージョン番号とが記録された記録媒体が配布され、記録装置1100は、
10 この記録媒体から鍵無効化データとバージョン番号とを読み出すとしてもよい。

次に、記録装置1100の比較部1108は、ドライブ部1110を介して、記録媒体1300の記録領域1305に鍵無効化データファイルが存在するか否かを確認する。鍵無効化データファイルが存在しないと確認された場合は（ステップS1502）、後述するステップS1505aに進む。

- 15 鍵無効化データファイル310が存在すると確認された場合は（ステップS1502）、比較部1108は、存在する全ての鍵無効化データファイルの版数記録部に記録されているバージョン番号について、ステップS1501で入手した鍵無効化データに付加されたバージョン番号と同じ内容のものが存在するか否かを確認する（ステップS1503）。

- 20 ステップS1503において、上記条件を満たすバージョン番号が存在しない場合は（ステップS1504）、後述するステップS1505aに進む。

ステップS1504において、上記条件を満たすバージョン番号が存在する場合は（ステップS1504）、制御部1109は、ドライブ部1110を介して、上記条件を満たすバージョン番号を含む鍵無効化データファイル1310の識別子記録部1312より、鍵無効化データ識別子RIDを読み出す（ステップS1505）。

- 25 鍵計算部1103は、デバイス鍵格納部101からデバイス鍵を読み出し、無効化データ格納部1102から鍵無効化データを読み出し（ステップS1506）、読み出した鍵無効化データを読み出したデバイス鍵で復号することによりメディア鍵MKを算出する（ステップS1507）。
- 30

次に、暗号化部1105は、算出されたメディア鍵を用いて、コンテンツサーバ装置1500から受信したコンテンツ鍵CKを暗号化して、暗号化コンテンツ鍵ECKを生成する（ステップS1508）。

5 認証子生成部1104は、記録媒体1300の固有番号記録領域1301から媒体固有番号MIDを読み出し（ステップS1509）、鍵計算部1103により算出されたメディア鍵MKと、暗号化部1105により生成された暗号化コンテンツ鍵ECKと、読み出した媒体固有番号MIDとを結合した値をハッシュ関数の入力値としたときの出力値として、認証子MACを生成する（ステップS1510）。なお、ここで使用するハッシュ関数は、公知の技術で実現可能である。例えばハッシュ関数としてSHA-1を使用するとしてもよい。
10 なお、SHA-1には限定されない。

次に、暗号化部1106は、コンテンツサーバ装置1500から受信したコンテンツ鍵CKを用いて、同じく受信したコンテンツCNTを暗号化する（ステップS1511）。

15 記録装置1100は、ステップS1505で取得した、又はステップS1505aで割当てられた鍵無効化データ識別子RIDと、ステップS1510で生成した認証子MACと、ステップS1508で生成した暗号化コンテンツ鍵と、ステップS1511で生成した暗号化コンテンツとを含む暗号化コンテンツファイルを、記録媒体1300の記録領域1305に記録し（ステップS1512）、処理を終了する。
20

また、記録媒体1300に鍵無効化データファイル1310が存在しないと確認された場合（ステップS1502）、及びステップS1503において条件を満たすバージョン番号が存在しない場合は（ステップS1504）、割当部1107は、ステップS1501で入手した鍵無効化データに対して、記録
25 媒体1300の記録領域1305に記録されている全ての鍵無効化データファイルに既に割当てられた鍵無効化データ識別子RIDとは異なる値を、鍵無効化データ識別子として、割当てる（ステップS1505a）。

例えば、記録媒体1300に、鍵無効化データファイルが一切存在しない場合には、割当部1107は、任意の値、例えば「1」を割当る。また、図14
30 に示す例のように、記録媒体1300aに、鍵無効化データ識別子RIDが「1」

及び「2」の鍵無効化データファイル1及び2が存在する場合には、割当部1107は、「1」及び「2」とは異なる値、例えば「3」を割当てる。

次に、記録装置1100のドライブ部1110は、ステップS1501で入手した鍵無効化データと、その鍵無効化データのバージョン番号と、ステップ
5 S1505aで割当てられた鍵無効化データ識別子とを有する鍵無効化データ
ファイルを、記録媒体1300の鍵無効化データファイル1302に記録する
(ステップS1505b)。このとき、鍵無効化データ、バージョン番号及び
鍵無効化データ識別子R I Dを、それぞれ、鍵無効化データファイル310の
データ記録部1313、版数記録部1311及び識別子記録部1312に記録
10 する。次に、ステップS1506へ制御が移り、以降、前述したステップS1
506からステップS1512までが実行される。

(2) 再生装置1200による再生の動作

再生装置1200による記録媒体1300に記録されているデータの再生の動作について、図19～図20に示すフローチャートを用いて説明する。

15 再生装置1200の指定受付部1207は、再生すべきコンテンツの指定を受け付ける(ステップS1601)。

取得部1208は、記録媒体1300の記録領域1305より、ステップS1601で指定されたコンテンツに対応する暗号化コンテンツファイルを見出す(ステップS1602)。

20 なお、指定受付部1207における再生すべきコンテンツの指定方法、及び、指定されたコンテンツに対応する暗号化コンテンツファイルの見出し方法としては、例えば、再生装置1200は、記録媒体1300の記録領域1305に記録されている全ての暗号化コンテンツファイルの属性を示す情報(例えば、暗号化コンテンツのファイル名、コンテンツのタイトル名、コンテンツの記録
25 日時、コンテンツの要約情報、コンテンツのサムネイル画像、コンテンツを示すアイコンなど)の一覧を、再生装置1200の表示部1217に表示し、利用者に、その一覧の中から、再生したいコンテンツを選択させることにより、再生すべきコンテンツの指定を受け付ける。また、再生装置1200は、指定されたコンテンツの属性情報から、指定されたコンテンツが格納された暗号化
30 コンテンツファイルのファイル名を知り、記録媒体1300の記録領域130

5から、該当のファイル名の暗号化コンテンツファイルを見出す。

なお、暗号化コンテンツファイルの見出し方法としては、上述の方法に限定されるものではなく、他の方法を用いてもよい。

取得部1208は、ステップS1602で見出した暗号化コンテンツファイル1320の識別子記録部1321より鍵無効化データ識別子を読み出す（ステップS1603）。

検索部1209は、記録媒体1300の記録領域1305より、ステップS1603で読み出した鍵無効化データ識別子R I Dと同じ値が、識別子記録部1312に記録されている鍵無効化データファイル310を見出す（ステップS1604）。次に、検索部1209は、ステップS1604で見出した鍵無効化データファイル1310を取得する（ステップS1605）。

鍵計算部1202は、デバイス鍵格納部1201からデバイス鍵を読み出し、検索部1209から鍵無効化データを受け取る（ステップS1606）。

鍵計算部1202は、ステップS1606で受け取った鍵無効化データを、デバイス鍵を用いて復号することにより復号メディア鍵 y を算出する（ステップS1607）。

認証子生成部1203は、記録媒体1300の固有番号記録領域1301から媒体固有番号M I Dを読み出し（ステップS1608）、ステップS1602で見出した暗号化コンテンツファイル1320の鍵記録部1323より暗号化コンテンツ鍵E C Kを読み出し（ステップS1609）、ステップS1607で取得した復号メディア鍵 y と、ステップS1609で読み出した暗号化コンテンツ鍵E C Kと、ステップS1608で取得した媒体固有番号M I Dとを結合した値をハッシュ関数の入力値としたときの出力値として、復号認証子D M A Cを生成する（ステップS1610）。ここで使用するハッシュ関数は、記録装置1100で用いたものと同じハッシュ関数S H A - 1である。

比較部1206は、ステップS1602で見出した暗号化コンテンツファイル1320の認証子記録部322より、認証子M A Cを読み出し（ステップS1611）、ステップS1610で算出された復号認証子D M A CとステップS1611で読み出した認証子M A Cが一致するかどうか確認する（ステップS1612）。

復号認証子DMACと認証子MACとが一致しなければ（ステップS1613）、再生動作は、終了する。

復号認証子DMACと認証子MACとが一致すれば（ステップS1613）、復号部1204は、暗号化コンテンツ鍵を、ステップS1607で算出した復号メディア鍵yで復号し、復号コンテンツ鍵DCKを取得する（ステップS1614）。

復号部1205は、ステップS1602で見出した暗号化コンテンツファイル1320のコンテンツ記録部1324より、暗号化コンテンツを読み出し（ステップS1615）、ステップS1615で読み出した暗号化コンテンツを、ステップS1614で復号した復号コンテンツ鍵DCKを用いて、復号して復号コンテンツし、再生部1214は、復号コンテンツを再生する（ステップS1616）。

2. 9 その他の変形例

以下に示すように構成してもよい。

（1）第2の実施の形態においては、鍵無効化データの世代を示すバージョン番号及び鍵無効化データを識別する鍵無効化データ識別子を、それぞれ、鍵無効化データファイルにおける版数記録部及び識別子記録部に記録するとしたが、この方法に限定されない。

例えば、鍵無効化データファイルを識別するファイル名の一部に、鍵無効化データのバージョン番号と鍵無効化データ識別子の両者、又は少なくとも1つを含む構成としても良い。具体的には、鍵無効化データファイルのファイル名を、“KRD__n__m”としてもよい。ここで、nはバージョン番号であり、mは鍵無効化データ識別子である。この場合、例えば、“KRD__0001__0002”というファイル名により識別される鍵無効化データファイルのバージョン番号は「1」であり、鍵無効化データ識別子RIDは「2」である。

このようにファイル名にバージョン番号や鍵無効化データ識別子の両者、又は少なくとも1つ含めることにより、再生装置は、ファイル名を見れば、鍵無効化データファイルのバージョン番号や鍵無効化データ識別子RIDを知ることができ、再生装置におけるファイルを検索する際の処理が軽減できるというメリットがある。

(2) 第2の実施の形態においては、鍵無効化データ識別子を、暗号化コンテンツファイルにおける識別子記録部に記録するとしたが、この方法に限定されない。

例えば、暗号化コンテンツファイルを識別するファイル名の一部に鍵無効化データ識別子を含める構成としても良い。具体的には、暗号化コンテンツを識別するファイル名を、“ECNT_m”としてもよい。ここで、mは、鍵無効化データ識別子である。例えば“ECNT_0002”というファイル名の暗号化コンテンツファイルの鍵無効化データ識別子RIDは「2」である。

このようにファイル名に鍵無効化データ識別子を含めることにより、再生装置において、ファイル名を見れば、鍵無効化データ識別子を知ることができ、再生装置における鍵無効化データ識別子の取得する際の処理が軽減できるというメリットがある。

(3) 第2の実施の形態においては、鍵無効化データを鍵無効化データ識別子と関連づけるため、また暗号化コンテンツを前記鍵無効化データ識別子RIDと関連づけるために、鍵無効化データファイル1310に、版数記録部1311と、識別子記録部1312を設け、それぞれ、バージョン番号と鍵無効化データ識別子とを記録し、暗号化コンテンツファイル1320に識別子記録部1321を設け、鍵無効化データ識別子を記録する構成としているが、この構成に限定されない。

例えば、記録装置は、記録媒体1300上に、1個以上の鍵無効化データファイルと、1個以上の暗号化コンテンツファイルと、1個の鍵無効化データ管理ファイルとを記録するとしてもよい。この鍵無効化データ管理ファイルには、鍵無効化データファイル毎に、その鍵無効化データのバージョン番号と、鍵無効化データ識別子と、記録媒体上で該鍵無効化データファイルを一意に特定するための情報（例えば、鍵無効化データファイルが記録されているディレクトリ名やファイル名など）と、該鍵無効化データファイルを用いて暗号化した暗号化コンテンツファイルを記録媒体上で一意に特定するための情報（例えば、暗号化コンテンツファイルが記録されているディレクトリ名やファイル名など）とが含まれる。再生装置は、この鍵無効化データ管理ファイルに記録されている上記情報に基づいて、再生が指定された暗号化コンテンツに関連する鍵

無効化データファイルを取得する。

また、本実施の形態の構成と、鍵無効化データ管理ファイルを設ける構成を組み合わせた構成としても良い。

(4) 第2の実施の形態では、鍵無効化データのバージョン番号と、鍵無効化データ識別子の両方が存在する構成としたが、この構成には限定されず、鍵無効化データ識別子だけが存在する構成でもよい。

(5) 第2の実施の形態では、鍵無効化技術として、記録媒体の書き換え可能領域に記録する鍵無効化データを、無効化されていない装置が保有するデバイス鍵を用いてメディア鍵を暗号化したものと、無効化された装置が保有するデバイス鍵を用いてメディア鍵とは無関係な値（例えば「0」）を暗号化したものとし、記録媒体の書き換え可能領域に記録する暗号化コンテンツを、コンテンツを前記メディア鍵に基づいて暗号化したものとする場合について説明したが、この構成に限定されるものではない。

例えば、記録媒体の書き換え可能領域に記録する鍵無効化データと暗号化コンテンツとして、無効化されていない装置においては、鍵無効化データに基づいて暗号化コンテンツが復号再生でき、無効化された装置においては、鍵無効化データに基づいて暗号化コンテンツが復号再生できないという条件を満たすものであればどんな構成であってもよい。

(6) 第2の実施の形態では、メディアバインド技術として、記録装置1100において媒体固有番号MIDを用いて認証子MACを生成して、再生装置1200において認証子MACの比較を行うとしているが、この構成に限定されるものではない。

例えば、記録装置1100において媒体固有番号MIDを用いてコンテンツを暗号化して記録媒体に記録し、再生装置1200において媒体固有番号MIDを用いて暗号化されたコンテンツを復号する構成としても良い。

(7) 第2の実施の形態では、鍵無効化データ識別子を割り当てる際、記録装置1100に既に記録されている鍵無効化データに割り当てられていない値を、鍵無効化IDとして割り当てる構成としているが、この構成に限定されるものではない。

例えば、記録装置1100は、既に割り当てた鍵無効化データ識別子を媒体固

有番号MIDとともに記憶しておき、記録装置1100に記憶している上記情報に基づいて、鍵無効化データ識別子を割り当てる構成としても良い。

2. 10 まとめ

以上の説明から明らかなように、本発明に係る記録装置は、特定装置が保有する鍵を無効化するための鍵無効化データを格納する鍵無効化データ格納手段と、前記鍵無効化データに基づいて前記コンテンツを暗号化するコンテンツ暗号化手段と、前記鍵無効化データに対して、前記記録媒体において前記鍵無効化データを一意に識別するための鍵無効化データ識別情報を割り当てる鍵無効化データ識別情報割当手段と、前記記録媒体に、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ記録手段と、前記暗号化コンテンツを前記鍵無効化データ識別情報と関連づけて記録する暗号化コンテンツ記録手段とを備える。

また、本発明の記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データに既に割当てられた鍵無効化データ識別情報とは異なる値を、鍵無効化データ識別情報情報として割当てる。

また、本発明の記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データと、前記鍵無効化データ格納手段に格納されている鍵無効化データの新旧を比較し、前記鍵無効化データ格納手段に格納されている鍵無効化データが新しい場合のみ、鍵無効化データ識別情報の割当てを行うことを特徴とする。

また、本発明における記録装置における前記鍵無効化データ識別情報割当手段は、前記記録媒体に記録されている鍵無効化データと、前記鍵無効化データ格納手段に格納されている鍵無効化データの新旧の比較を、各鍵無効化データが生成された日時に関連する情報、もしくは、各鍵無効化データが生成された順序に関連する情報に基づいて行う。

また、本発明に係る再生装置は、前記記録媒体から、暗号化コンテンツと、前記暗号化コンテンツに関連づけて記録された鍵無効化データ識別情報を読み出す暗号化コンテンツ読出手段と、前記記録媒体から、前記暗号化コンテンツ読出手段にて読み出した鍵無効化データ識別情報と同じ鍵無効化データ識別情報が関連づけて記録されている鍵無効化データを読み出す鍵無効化データ読出

手段と、前記鍵無効化データ読出手段にて読み出した鍵無効化データに基づいて前記暗号化コンテンツ読出手段で読み出した前記暗号化コンテンツを復号するコンテンツ復号手段とを備える。

- 5 また、本発明における記録媒体は、鍵無効化データを、前記記録媒体においてこの鍵無効化データを一意に識別するための鍵無効化データ識別情報と関連づけて記録する鍵無効化データ格納手段と、前記鍵無効化データに基づいて暗号化された暗号化コンテンツを前記無効化データ識別情報と関連づけて記録する暗号化コンテンツ格納手段とを備える。

- 10 また、本発明における前記記録媒体は、さらに、鍵無効化データの新旧を示す情報を、鍵無効化データと関連づけて記録する。

- また、本発明における著作権保護システムは、記録装置と、記録媒体と、再生装置からなり、前記記録装置は、特定装置が保有する鍵を無効化するための鍵無効化データを格納する鍵無効化データ格納手段と、前記鍵無効化データに基づいて前記コンテンツを暗号化するコンテンツ暗号化手段と、前記鍵無効化
- 15 データに対して、前記記録媒体において前記鍵無効化データを一意に識別するための鍵無効化データ識別情報を割当てる鍵無効化データ識別情報割当手段と、前記記録媒体に、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ記録手段と、前記暗号化コンテンツを前記鍵無効化データ識別情報と関連づけて記録する暗号化コンテンツ記録手段とを備え、
- 20 前記記録媒体は、前記鍵無効化データを前記鍵無効化データ識別情報と関連づけて記録する鍵無効化データ格納手段と、前記暗号化コンテンツを前記無効化データ識別情報と関連づけて記録する暗号化コンテンツ格納手段とを備え、前記再生装置は、前記記録媒体から、暗号化コンテンツと、前記暗号化コンテンツに関連づけて記録された鍵無効化データ識別情報を読み出す暗号化コンテンツ
- 25 ツ読出手段と、前記暗号化コンテンツ読出手段にて読み出した鍵無効化データ識別情報と同じ鍵無効化データ識別情報が関連づけて記録されている鍵無効化データを読み出す鍵無効化データ読出手段と、前記鍵無効化データ読出手段にて読み出した鍵無効化データに基づいて前記暗号化コンテンツ読出手段で読み出した前記暗号化コンテンツを復号するコンテンツ復号手段とを備える。

- 30 このように、第2の実施の形態に係る記録装置、記録媒体、再生装置、及び、

著作権保護システムにおいては、記録媒体に記録する鍵無効化データに対して、記録媒体においてその鍵無効化データを一意に識別するための鍵無効化データ I D を割当て、この鍵無効化データ I D を、記録媒体に記録する鍵無効化データと関連づけて鍵無効化データファイルとして記録するとともに、この鍵無効化データ I D を、該鍵無効化データを使用して暗号化したコンテンツと関連づけて、暗号化コンテンツファイルとして、記録することにより、再生装置において、該暗号化コンテンツを復号再生する場合に、記録媒体に、複数の暗号化コンテンツファイルと、複数の鍵無効化データファイルが記録されている場合においても、該暗号化コンテンツファイルに含まれる鍵無効化データ I D と同じ鍵無効化データ I D を含む鍵無効化データファイルを検索取得することができ、暗号化コンテンツファイルを取得した鍵無効化データファイルを用いて復号再生することが可能となる。

3. その他の変形例

なお、本発明を上記の各実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 各実施の形態において、コンテンツは、映像データと音声データとが高効率で圧縮符号化されたデータであるとしているが、これには、限定されない。例えば、コンテンツは、小説、静止画像、音声などがデジタル化されたコンピュータデータであるとしてもよい。

また、例えば、コンテンツは、コンピュータを構成するマイクロプロセッサの動作を制御する複数の命令から構成されるコンピュータプログラムであるとしてもよい。また、表計算ソフトにより生成される表データであるとしてもよいし、データベースソフトにより生成されるデータベースであるとしてもよい。

(2) 上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。

(3) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

10 また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、
15 前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより
20 実施するとしてもよい。

(4) 上記各実施の形態及び上記各変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用の可能性

25 本発明を構成する各装置及び記録媒体は、コンテンツを制作し、配給するコンテンツ配給産業において、経営的に、また継続的及び反復的に使用することができる。また、本発明を構成する各装置及び記録媒体は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。

請 求 の 範 囲

1. 記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムであって、

前記複数の再生装置のうちいずれか1台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

10 前記記録装置は、

無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、

15 前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出手段と、

読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成手段と、

20 生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化手段と、

前記記憶手段から前記メディア鍵データを読み出す読出手段と、

読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込手段とを備え、

各再生装置は、

25 前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出手段と、

当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号手段と、

生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検

知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御手段と、

復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段と

を備えることを特徴とする著作物保護システム。

2. 記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記記録装置であって、

前記複数の再生装置のうちいずれか1台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、

無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段と、

前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出手段と、

読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成手段と、

生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化手段と、

前記記憶手段から前記メディア鍵データを読み出す読出手段と、

読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込手段と

を備えることを特徴とする記録装置。

3. 別の記録媒体は、無効化されていない各再生装置についてメディア鍵が、

無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の別の暗号化メディア鍵から構成される別のメディア鍵データを記憶しており、

前記記録装置は、さらに、

- 5 前記別の記録媒体に記憶されている別のメディア鍵データと、前記記憶手段に記憶されている前記メディア鍵データとの新旧を比較する比較手段と、

前記別のメディア鍵データの方が新しいと判断される場合に、前記別の記録媒体から前記別のメディア鍵データを読み出し、読み出した前記別のメディア鍵データを、前記記憶手段に記憶されている前記メディア鍵データに、上書き

- 10 する更新手段とを備え、

前記読出手段は、前記メディア鍵データの読出しに代えて、前記記憶手段から前記別のメディア鍵データを読み出し、

前記書込手段は、前記メディア鍵データの書込みに代えて、読み出された前記別のメディア鍵データを前記記録媒体の前記書換可能領域に書き込む

- 15 ことを特徴とする請求の範囲2に記載の記録装置。

4. 前記記憶手段に記憶されている前記メディア鍵データは、当該メディア鍵データの世代を示す第1バージョン情報を含み、

前記別の記録媒体に記憶されている前記別のメディア鍵データは、当該別のメディア鍵データの世代を示す第2バージョン情報を含み、

- 20 前記比較手段は、前記第1バージョン情報と前記第2バージョン情報とを比較することにより、前記別のメディア鍵データと前記メディア鍵データとの新旧を比較する

ことを特徴とする請求の範囲3に記載の記録装置。

- 25 5. 前記記憶手段に記憶されている前記メディア鍵データは、当該メディア鍵データが生成された日時を示す第1日時情報を含み、

前記別の記録媒体に記憶されている前記別のメディア鍵データは、当該別のメディア鍵データが生成された日時を示す第2日時情報を含み、

前記比較手段は、前記第1日時情報と前記第2日時情報とを比較することにより、前記別のメディア鍵データと前記メディア鍵データとの新旧を比較する

- 30 ことを特徴とする請求の範囲3に記載の記録装置。

6. 前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、

前記記録装置は、さらに、前記無効化データに対してデジタル署名を施して

5 検証情報を生成する署名生成手段を備え、

前記書込手段は、さらに、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込む

ことを特徴とする請求の範囲2に記載の記録装置。

7. 前記署名生成手段は、前記無効化データに対して、付録型の前記デジタル
10 署名を施して署名データを生成し、生成した前記署名データと前記無効化データとから構成される前記検証情報を生成し、

前記書込手段は、前記署名データと前記無効化データとから構成される前記検証情報を書き込む

ことを特徴とする請求の範囲6に記載の記録装置。

15 8. 前記署名生成手段は、前記無効化データに対して、回復型の前記デジタル署名を施して前記検証情報を生成する

ことを特徴とする請求の範囲6に記載の記録装置。

9. 前記記憶手段は、さらに、当該記録装置の秘密鍵と公開鍵証明書とを記憶しており、

20 前記署名生成手段は、前記記憶手段に記憶されている前記秘密鍵を用いて、前記デジタル署名を施し、

前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、

前記書込手段は、読み出された前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込む

25 ことを特徴とする請求の範囲6に記載の記録装置。

10. 前記記憶手段は、さらに、当該記録装置の公開鍵証明書を記憶しており、

前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、

前記書込手段は、読み出された前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込む

30 ことを特徴とする請求の範囲2に記載の記録装置。

1 1. 前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、

前記記録装置は、さらに、前記無効化データに対してデジタル署名を施して
5 検証情報を生成する署名生成手段を備え、

前記書込手段は、さらに、生成した前記検証情報を別の記録媒体に書き込むことを特徴とする請求の範囲2に記載の記録装置。

1 2. 前記記憶手段は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶
10 しており、

前記読出手段は、さらに、前記記憶手段から前記無効化データを読み出し、
前記書込手段は、読み出された前記無効化データを別の記録媒体に書き込むことを特徴とする請求の範囲2に記載の記録装置。

1 3. 前記記憶手段は、さらに、当該記録装置の公開鍵証明書を記憶しており、
15 前記読出手段は、さらに、前記記憶手段から前記公開鍵証明書を読み出し、
前記書込手段は、読み出された前記公開鍵証明書を別の記録媒体に書き込むことを特徴とする請求の範囲2に記載の記録装置。

1 4. 前記記憶手段は、さらに、当該記録装置を識別する装置識別子を記憶し
20 ており、
前記記録装置は、さらに、

前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記コンテンツに電子透かしとして埋め込む埋込手段を備え、

前記暗号化手段は、前記装置識別子が埋め込まれたコンテンツを暗号化することを特徴とする請求の範囲2に記載の記録装置。

25 1 5. 前記記憶手段に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、

前記書込手段は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換可能領域に書き込む

30 ことを特徴とする請求の範囲2に記載の記録装置。

16. 前記記録媒体は、さらに、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の別の暗号化メディア鍵から構成される別のメディア鍵データを記憶しており、前記別のメディア鍵データは、当該メディア鍵データを識別する別のデータ識別子を含み、前記記録装置は、さらに、

前記記録媒体に記録されている別のメディア鍵データを識別する前記別のデータ識別子とは、異なる前記データ識別子を前記記憶手段に記憶されている前記メディア鍵データに割り当てる割当手段を含む

10 ことを特徴とする請求の範囲15に記載の記録装置。

17. 前記記録媒体は、さらに、

前記記憶手段に記憶されている前記メディア鍵データと、前記記録媒体に記録されている前記別のメディア鍵データとの新旧を比較する比較手段を含み、

15 前記割当手段は、前記記憶手段に記憶されている前記メディア鍵データの方が新しいと判断される場合に、前記データ識別子を割り当てる

ことを特徴とする請求の範囲15に記載の記録装置。

18. 前記記憶手段に記憶されている前記メディア鍵データは、当該メディア鍵データが生成された日時を示す第1日時情報を含み、

20 前記記録媒体に記憶されている前記別のメディア鍵データは、当該別のメディア鍵データが生成された日時を示す第2日時情報を含み、

前記比較手段は、前記第1日時情報と前記第2日時情報とを比較することにより、前記別のメディア鍵データと前記メディア鍵データとの新旧を比較することを特徴とする請求の範囲17に記載の記録装置。

25 19. 記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記再生装置であって、

前記複数の再生装置のうちいずれか1台以上は、無効化されており、

30 前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されけるメディア鍵データを記憶しており、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出し、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成し、前記記憶手段から前記メディア鍵データを読み出し、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込み、

前記再生装置は、

前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出手段と、

当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号手段と、

生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御手段と、

復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号手段と

を備えることを特徴とする再生装置。

20. 前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記無効化データに対してデジタル署名を施して検証情報を生成し、生成した前記検証情報を前記記録媒体の前記書換可能領域に書き込み、

前記読出手段は、さらに、前記記録媒体の前記書換可能領域に書き込まれた前記検証情報を読み出し、

前記再生装置は、さらに、

読み出した前記検証情報に基づいて、署名検証を施して、検証の成功又は失敗を示す検証結果を出力する検証手段を備え、

前記制御手段は、さらに、前記検証結果が検証の失敗を示す場合に、前記暗号化コンテンツの復号を禁止し、前記検証結果が検証の成功を示す場合に、前

5 記暗号化コンテンツの復号を許可する

ことを特徴とする請求の範囲 19 に記載の再生装置。

21. 前記記録装置は、前記無効化データに対して、付録型の前記デジタル署名を施して署名データを生成し、生成した前記署名データと前記無効化データとから構成される前記検証情報を生成し、前記署名データと前記無効化データ
10 とから構成される前記検証情報を書き込み、

前記検証手段は、前記検証情報に含まれている前記署名データに基づいて、前記署名検証を施す

ことを特徴とする請求の範囲 20 に記載の再生装置。

22. 前記記録装置は、前記無効化データに対して、回復型の前記デジタル署名を施して前記検証情報を生成し、
15

前記検証手段は、検証結果が成功の場合に、前記検証情報から前記無効化データを生成する

ことを特徴とする請求の範囲 20 に記載の再生装置。

23. 前記記録装置は、さらに、当該記録装置の秘密鍵と公開鍵証明書とを記憶しており、記憶している前記秘密鍵を用いて、前記デジタル署名を施し、前記公開鍵証明書を読み出し、読み出した前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込み、
20

前記検証手段は、前記記録媒体から前記公開鍵証明書を読み出し、読み出した公開鍵証明書から公開鍵を抽出し、抽出した前記公開鍵を用いて、前記署名検証を施す
25

ことを特徴とする請求の範囲 20 に記載の再生装置。

24. 前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す無効化データを記憶しており、前記無効化データに対してデジタル署名を施して検証情報を生成
30 し、生成した前記検証情報を別の記録媒体に書き込み、

前記読出手段は、前記記録媒体からの前記検証情報の読み出しに代えて、前記別の記録媒体から前記検証情報を読み出し、

前記検証手段は、前記別の記録媒体から読み出した前記検証情報に基づいて、署名検証を施す

5 ことを特徴とする請求の範囲 20 に記載の再生装置。

25. 前記記録装置は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記公開鍵証明書を読み出し、読み出した前記公開鍵証明書を前記記録媒体の前記書換可能領域に書き込み、

前記再生装置は、さらに、

10 前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第 1 無効化データを記憶している記憶手段と、

前記記録媒体から前記公開鍵証明書を読み出す証明書読出手段と、

読み出した公開鍵証明書に含まれる公開鍵が、前記第 1 無効化データにより、無効化されていることを示しているか否かを検証する公開鍵検証手段とを含み、

15 前記制御手段は、さらに、前記公開鍵が無効化されている場合に、前記暗号化コンテンツの復号を禁止し、前記公開鍵が無効化されていない場合に、前記暗号化コンテンツの復号を許可する

ことを特徴とする請求の範囲 19 に記載の再生装置。

26. 別の記録媒体は、前記記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第 2 無効化データを記憶し
20 ており、

前記再生装置は、さらに、

前記別の記録媒体に記憶されている前記第 2 無効化データと、前記記憶手段に記憶されている前記第 1 無効化データとの新旧を比較する比較手段と、

25 前記第 2 無効化データの方が新しいと判断される場合に、前記別の記録媒体から前記第 2 無効化データを読み出し、読み出した前記第 2 無効化データを、前記記憶手段に記憶されている前記第 1 無効化データに、上書きする更新手段とを含む

ことを特徴とする請求の範囲 25 に記載の再生装置。

30 27. 前記比較手段は、前記第 1 無効化データのサイズと前記第 2 無効化デー

タのサイズとを比較することにより、前記第1無効化データと前記第2無効化データとの新旧を比較する

ことを特徴とする請求の範囲26に記載の再生装置。

28. 前記比較手段は、前記第1無効化データにより示される無効化された公開鍵の数と前記第2無効化データにより示される無効化された公開鍵の数とを比較することにより、前記第1無効化データと前記第2無効化データとの新旧を比較する

ことを特徴とする請求の範囲26に記載の再生装置。

29. 前記記憶手段に記憶されている前記第2無効化データは、当該第2無効化データの世代を示す第2バージョン情報を含み、

前記別の記録媒体に記憶されている前記第1無効化データは、当該第1無効化データの世代を示す第1バージョン情報を含み、

前記比較手段は、前記第1バージョン情報と前記第2バージョン情報とを比較することにより、前記第1無効化データと第2無効化データとの新旧を比較する

ことを特徴とする請求の範囲26に記載の再生装置。

30. 前記記憶手段に記憶されている前記第2無効化データは、当該第2無効化データが生成された日時を示す第2日時情報を含み、

前記別の記録媒体に記憶されている前記第1無効化データは、当該第1無効化データが生成された日時を示す第1日時情報を含み、

前記比較手段は、前記第1日時情報と前記第2日時情報とを比較することにより、前記第1無効化データと第2無効化データとの新旧を比較する

ことを特徴とする請求の範囲26に記載の再生装置。

31. 前記記録装置は、さらに、当該記録装置及び前記複数の再生装置のいずれかに割り当てられた公開鍵が無効化されていることを示す第2無効化データを記憶しており、前記第2無効化データを読み出し、読み出した前記第2無効化データを別の記録媒体に書き込み、

前記公開鍵検証手段は、前記第1無効化データに代えて、前記別の記録媒体から前記第2無効化データを読み出し、読み出した前記第2無効化データにより、前記公開鍵が無効化されていることを示しているか否かを検証する

ことを特徴とする請求の範囲 25 に記載の再生装置。

32. 前記記録装置は、さらに、当該記録装置の公開鍵証明書を記憶しており、前記公開鍵証明書を読み出し、読み出した前記公開鍵証明書を別の記録媒体に書き込み、

- 5 前記証明書読出手段は、前記記録媒体に代えて、前記別の記録媒体から前記公開鍵証明書を読み出す

ことを特徴とする請求の範囲 25 に記載の再生装置。

33. 前記再生装置は、さらに、

当該再生装置を識別する装置識別子を記憶している前記記憶手段と、

- 10 復号が許可された場合に、前記記憶手段から前記装置識別子を読み出し、読み出した前記装置識別子を前記暗号化コンテンツに電子透かしとして埋め込む埋込手段と、

前記装置識別子が埋め込まれた前記暗号化コンテンツを前記記録媒体に書き込む

- 15 ことを特徴とする請求の範囲 19 に記載の再生装置。

34. 前記記録装置に記憶されている前記メディア鍵データは、さらに、当該メディア鍵データを識別するデータ識別子を含み、前記記録装置は、前記データ識別子と前記暗号化コンテンツとを対応付けて、前記記録媒体の前記書換可能領域に書き込み、前記データ識別子を含む前記メディア鍵データを前記書換

- 20 可能領域に書き込み、

前記再生装置は、さらに、

前記記録媒体に記録されている前記暗号化コンテンツの指定を受け付ける受付手段と、

指定が受け付けられた前記暗号化コンテンツに対応付けられた前記データ識別子を前記記録媒体から読み出す読出手段と、

- 25

読み出した前記データ識別子を含む前記メディア鍵データを前記記録媒体から読み出す読出手段とを含み、

前記制御手段は、読み出した前記メディア鍵データに基づいて、前記暗号化コンテンツの復号の可否を判断する

- 30 ことを特徴とする請求の範囲 19 に記載の再生装置。

35. 記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記記録装置で用いられる記録方法であって、

5 前記複数の再生装置のうちいずれか1台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

10 前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されるメディア鍵データを記憶している記憶手段を備え、

前記記録方法は、

15 前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出ステップと、

読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成する生成ステップと、

生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化ステップと、

20 前記記憶手段から前記メディア鍵データを読み出す読出ステップと、

読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込む書込ステップと

を含むことを特徴とする記録方法。

25 36. 記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記記録装置で用いられる記録用のコンピュータプログラムであって、

前記複数の再生装置のうちいずれか1台以上は、無効化されており、

30 前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有

番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成

5 成されるメディア鍵データを記憶している記憶手段を備え、

前記記録用のコンピュータプログラムは、

前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出す読出ステップと、

読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生

10 成する生成ステップと、

生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成する暗号化ステップと、

前記記憶手段から前記メディア鍵データを読み出す読出ステップと、

読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを

15 前記記録媒体の前記書換可能領域に書き込む書込ステップと

を含むことを特徴とするコンピュータプログラム。

37. 前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求の範囲37に記載のコンピュータプログラム。

20 38. 記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記再生装置で用いられる再生方法であって、

前記複数の再生装置のうちいずれか1台以上は、無効化されており、

25 前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置の

30 デバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成

成されけるメディア鍵データを記憶しており、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出し、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成し、前記記憶手段から前記メディア鍵データを読み出し、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込み、

前記再生方法は、

前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出ステップと、

当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号ステップと、

生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御ステップと、

復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップと

を含むことを特徴とする再生方法。

39. 記録媒体にコンテンツを暗号化して書き込む記録装置と、前記記録媒体に記録されている暗号化コンテンツの復号を試みる複数の再生装置とから構成される著作物保護システムにおける前記再生装置で用いられる再生用のコンピュータプログラムであって、

前記複数の再生装置のうちいずれか1台以上は、無効化されており、

前記記録媒体は、読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

前記記録装置は、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置の

デバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア鍵から構成されけるメディア鍵データを記憶しており、前記記録媒体の前記書換不可領域から前記媒体固有番号を読み出し、読み出した前記媒体固有番号及び前記メディア鍵に基づいて、暗号化鍵を生成し、生成された前記暗号化鍵に基づいて、

5 デジタルデータであるコンテンツを暗号化して暗号化コンテンツを生成し、前記記憶手段から前記メディア鍵データを読み出し、読み出された前記メディア鍵データ及び生成された前記暗号化コンテンツを前記記録媒体の前記書換可能領域に書き込み、

前記再生用のコンピュータプログラムは、

- 10 前記記録媒体の前記書換可能領域に書き込まれたメディア鍵データから当該再生装置に対応する暗号化メディア鍵を読み出す読出ステップと、

当該再生装置のデバイス鍵を用いて、読み出された前記暗号化メディア鍵を復号して復号メディア鍵を生成する復号ステップと、

- 15 生成された復号メディア鍵が、前記検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止し、前記検知情報でない場合に、暗号化コンテンツの復号を許可する制御ステップと、

- 20 復号が許可された場合に、前記記録媒体から前記暗号化コンテンツを読み出し、生成された復号メディア鍵に基づいて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する復号ステップと

を含むことを特徴とするコンピュータプログラム。

40. 前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求の範囲39に記載のコンピュータプログラム。

- 25 41. コンピュータ読み取り可能な記録媒体であって、

読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録されており、

- 30 前記書換可能領域には、メディア鍵データと暗号化コンテンツとが記録され

ており、

前記メディア鍵データは、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア

5 鍵から構成され、

前記暗号化コンテンツは、暗号化鍵に基づいて、デジタルデータであるコンテンツを暗号化して生成したものであり、

前記暗号化鍵は、前記記録媒体の前記書換不可領域に記録されている前記媒体固有番号及び前記メディア鍵に基づいて、生成されたものである

10 ことを特徴とする記録媒体。

4 2. コンピュータ読み取り可能な記録媒体であって、

読出専用の書換不可領域と、読出し及び書込みの可能な書換可能領域とを備え、

前記書換不可領域には、当該記録媒体に固有の媒体固有番号が予め記録され
15 ており、

前記書換可能領域には、メディア鍵データと暗号化コンテンツとが記録されて
ており、

前記メディア鍵データは、無効化されていない各再生装置についてメディア
鍵が、無効化された各再生装置について所定の検知情報が、それぞれ、当該再
20 生装置のデバイス鍵を用いて、暗号化されて生成された複数の暗号化メディア
鍵から構成され、当該メディア鍵データを識別子するデータ識別子を含み、

前記暗号化コンテンツは、暗号化鍵に基づいて、デジタルデータであるコン
テンツを暗号化して生成したものであり、前記データ識別子を含み、

前記暗号化鍵は、前記記録媒体の前記書換不可領域に記録されている前記媒
25 体固有番号及び前記メディア鍵に基づいて、生成されたものである

ことを特徴とする記録媒体。

要 約 書

コンテンツの不正利用を防止することができる記録装置及び再生装置を提供する。

- 5 記録媒体は、書換不可領域に媒体固有番号を記録している。

記録装置は、メディア鍵データ及び暗号化コンテンツを前記記録媒体に書き込む。前記メディア鍵データは、無効化されていない各再生装置についてメディア鍵が、無効化された各再生装置について検知情報が、それぞれ、当該再生装置のデバイス鍵を用いて、暗号化されて生成され

- 10 た複数の暗号化メディア鍵から構成される。

再生装置は、デバイス鍵を用いて、暗号化メディア鍵を復号して復号メディア鍵を生成し、復号メディア鍵が、検知情報であるか否かを判断し、前記検知情報である場合に、前記記録媒体に記録されている暗号化コンテンツの復号を禁止する。